



System i

Справочник
Справочник по защите

Версия 6 выпуск 1

SC43-0358-10





System i

Справочник

Справочник по защите

Версия 6 выпуск 1

SC43-0358-10

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе Приложение I, “Примечания”, на стр. 769.

Это издание относится к версии 6, выпуску 1, модификации 0 IBM i5/OS (код продукта 5761-SS1) а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

Настоящее издание заменяет публикацию SC41-5302-09.

© Copyright International Business Machines Corporation 1996, 2008. Все права защищены.

Содержание

I Новое в V6R1 xi

Глава 1. Введение в защиту System i . . . 1

Физическая защита	2
Защита с помощью ключа	2
Уровень защиты	2
Системные значения	3
Цифровые подписи	3
Включение единого входа в систему	4
Пользовательские профайлы	4
Профайлы групп	5
Защита ресурсов	5
Журнал контроля за действиями	6
Среда защиты Common Criteria	7
Независимый пул дисков	7

Глава 2. Работа с системным значением Защита системы (QSecurity) 9

Уровень защиты 10	12
Уровень защиты 20	12
Переход с уровня 10 на уровень 20	13
Переход на уровень 20 с более высокого уровня	13
Уровень защиты 30	13
Переход на уровень 30 с более низкого уровня	13
Уровень защиты 40	14
Предотвращение использования неподдерживаемых интерфейсов	16
Защита описаний заданий	17
Вход в систему без ИД пользователя и пароля	17
Расширенная аппаратная защита памяти	18
Защита области программы	18
Защита адресного пространства задания	18
Проверка параметров	18
Проверка восстанавливаемых программ	18
Переход на уровень защиты 40	19
Выключение уровня защиты 40	20
Уровень защиты 50	20
Ограничения на объекты пользовательского домена	20
Ограничения на обработку сообщений	21
Запрет на изменение внутренних управляющих блоков	22
Переход на уровень защиты 50	22
Выключение уровня защиты 50	22

Глава 3. Системные значения защиты 25

Общие системные значения защиты	26
Разрешить объекты пользовательского домена (QALWUSRDMN)	27
Права доступа к новым объектам (QCRTAUT)	28
Показать информацию о входе в систему (QDSPSGNINF)	29
Тайм-аут для неактивного задания (QINACTITV)	29
Очередь сообщений неактивного задания (QINACTMSGQ)	30

Ограничить сеансы одним устройством (QLMTDEVSSN)	31
Ограничить права доступа системного администратора (QLMTSECOFR)	32
Максимальное число попыток входа в систему (QMAXSIGN)	32
Действие при достижении максимального числа попыток входа в систему (QMAXSGNACN)	33
Сохранить идентификационные данные на сервере (QRETSVRSEC)	34
Удаленное включение и перезапуск (QRMTIPL)	34
Управление удаленным входом в систему (QRMTSIGN)	35
Сканирование в файловых системах (QSCANFS)	36
Управление сканированием в файловых системах (QSCANFCTL)	36
Управление общей памятью (QSHRMEMCTL)	38
Применять принятые права доступа (QUSEADPAUT)	38
Системные значения, связанные с защитой	39
Автоматическая настройка устройств (QAUTOCFG)	40
Автоматическая настройка виртуальных устройств (QAUTOVRT)	40
Действие по восстановлению устройства (QDEVRCYACN)	41
Тайм-аут для отключенного задания (QDSCJOBITV)	42
Атрибут удаленного обслуживания (QRMTSRVATR)	42
Список шифров Secure Sockets Layer (SSL) (QSSLCSL)	43
Управление шифрами Secure Sockets Layer (SSL) (QSSLCSLCTL)	43
Протоколы Secure Sockets Layer (SSL) (QSSLPCL)	44
Системные значения восстановления, связанные с защитой	44
Проверять восстанавливаемые объекты (QVFYOBJRST)	45
Преобразование при восстановлении (QFRCCVNRST)	47
Разрешить восстановление конфиденциальных значений (QALWOBJRST)	48
Системные значения, связанные с паролями	49
Блокировка изменения пароля (QPWDCHGBLK)	51
Срок действия пароля (QPWDEXPITV)	51
Предупреждение об истечении срока действия пароля (QPWDEXPWRN)	52
Уровень пароля (QPWDLVL)	52
Минимальная длина пароля (QPWDMINLEN)	53
Максимальная длина пароля (QPWDMAXLEN)	54
Обязательное изменение пароля (QPWDRQDDIF)	54
Запретить некоторые символы в пароле (QPWDLMTCHR)	55
Запретить применение последовательности цифр (QPWDLMTAJC)	55

Запретить применение повторяющихся символов (QPWDLMTREP)	56	Очередь сообщений	106
Запретить символы в одинаковых позициях (QPWDPOSDIF)	57	Доставка	107
Обязательное вхождение в пароль цифр (QPWDRQDDGT)	57	Серьезность	108
Правила паролей (QPWDRULES)	57	Принтер	108
Программа подтверждения паролей (QPWDVLDPGM)	63	Очереди вывода	108
Работа с программой подтверждения паролей	64	Программа обработки клавиши Attention	109
Системные значения, связанные с контролем	68	Последовательность сортировки	110
Управление контролем (QAUDCTL)	69	Идентификатор языка	111
Действие при сбое контроля (QAUDENDACN)	69	Идентификатор страны или региона	111
Число записей в журнале контроля перед их сохранением (QAUDFRCLVL)	70	Идентификатор набора символов	111
Уровень контроля (QAUDLVL)	71	Управляющий элемент символического идентификатора	112
Расширение уровня контроля (QAUDLVL2)	72	Атрибуты задания	112
Контроль за новыми объектами (QCRTOBJAUD)	74	Локаль	113
		Опции пользователя	113
		Идентификатор пользователя	114
		Номер ИД группы	114
		Домашний каталог	115
		Связь EIM	115
		Права доступа	116
		Контроль объекта	117
		Контроль действий	118
		Дополнительная информация, связанная с пользовательскими профайлами	120
		Частные права доступа	120
		Права доступа основной группы	121
		Информация о принадлежности объекта	121
		Цифровой идентификатор	121
		Работа с пользовательскими профайлами	122
		Создание пользовательского профайла	122
		Применение команды Работа с пользовательскими профайлами	122
		Применение команды Создать пользовательский профайл	123
		Применение опции Работа с регистрацией пользователей	123
		Копирование пользовательского профайла	124
		Копирование с помощью меню Работа с пользовательскими профайлами	125
		Копирование с помощью меню Работа с регистрацией пользователей	126
		Копирование частных прав доступа	127
		Изменение пользовательского профайла	127
		Удаление пользовательских профайлов	127
		Применение команды Удалить пользовательский профайл	127
		Применение опции Удалить пользователя	128
		Работа с объектами по частным правам доступа	129
		Работа с объектами по основной группе	129
		Включение пользовательского профайла	129
		Просмотр пользовательских профайлов	130
		Просмотр отдельного профайла	130
		Просмотр всех профайлов	130
		Тип показа пользовательского профайла	131
		Типы отчетов пользовательского профайла	131
		Переименование пользовательского профайла	131
		Работа со средствами контроля пользователей	132
		Работа с профайлами в программах CL	133
		Точки выхода пользовательского профайла	133
		IBM, поставляемые пользовательские профайлы	133
Глава 4. Пользовательские профайлы	77		
Роли пользовательских профайлов	77		
Профайлы групп	78		
Поля параметров пользовательского профайла	78		
Пользовательский профайл	79		
Пароль	80		
Ограничить срок действия пароля	82		
Состояние	83		
Класс пользователя	83		
Уровень поддержки	84		
Текущая библиотека	85		
Начальная программа	86		
Начальное меню	87		
Ограничить возможности	87		
Описание	89		
Специальные права доступа	89		
*ALLOBJ, специальные права доступа	90		
Специальные права доступа *SECADM	90		
Специальные права доступа *JOBCTL	91		
Специальные права доступа *SPLCTL	91		
Специальные права доступа *SAVSYS	91		
Специальные права доступа *SERVICE	92		
Предоставление доступа к трассировке	92		
Специальные права доступа *AUDIT	93		
Специальные права доступа *IOSYSCFG	94		
Специальная среда	94		
Показать информацию о входе в систему	95		
Срок действия пароля	96		
Блокировка изменения пароля	97		
Локальное управление паролем	97		
Ограничить сеансы одним устройством	98		
Буферизация нажатий клавиш	98		
Максимальный объем памяти	99		
Ограничение приоритета	100		
Описание задания	101		
Профайл группы	102		
Владелец	102		
Права доступа группы	103		
Тип прав доступа группы	104		
Дополнительные группы	104		
Код учета ресурсов	105		
Пароль документов	106		

Изменение паролей для пользовательских профайлов, поставляемых IBM	134	Настройка списка прав доступа для защиты объектов	175
Работа с ИД пользователей сервисных средств	135	Настройка списка прав доступа	176
Системный пароль	135	Удаление списка прав доступа	177
Глава 5. Защита ресурсов	137	Как система проверяет права доступа	177
Определение субъектов доступа к информации	137	Блок-схемы проверки прав доступа	178
Определение режима доступа к информации	138	Блок-схема 1: Основной процесс проверки прав доступа	178
Часто используемые права доступа	139	Блок-схема 2: Быстрая проверка прав доступа к объекту	180
Определение условий доступа к информации	141	Блок-схема 3: Проверка прав доступа пользователя к объекту	182
Защита библиотек	141	Блок-схема 4: Проверка прав доступа владельца	184
Защита библиотек и списки библиотек	142	Блок-схема 5: Быстрая проверка прав доступа пользователя	185
Права доступа к полям	142	Блок-схема 6: Проверка прав доступа группы	188
Защита при работе со средой System/38	144	Блок-схема 7: Проверка общих прав доступа	190
Рекомендации по применению среды System/38 Environment	144	Блок-схема 8: Проверка принятых прав доступа	191
Защита каталога	144	Примеры проверки прав доступа	195
Защита списка прав доступа	144	Пример 1: Применение частных прав доступа группы	195
Управление списком прав доступа	145	Пример 2: Применение прав доступа основной группы	196
Применение списка прав доступа для защиты объектов, поставляемых IBM	145	Пример 3: Применение общих прав доступа	198
Права доступа к новым объектам библиотеки	146	Пример 4: Применение общих прав доступа без поиска частных прав доступа	198
Опасность применения прав, устанавливаемых при создании (CRTAUT)	146	Пример 5: Применение принятых прав доступа	199
Права доступа к новым объектам каталога	147	Пример 6: Права доступа пользователя и группы	200
Принадлежность объекта	149	Пример 7: Общие права доступа без частных прав доступа	201
Групповая принадлежность объектов	150	Пример 8: Принятые права доступа без частных прав доступа	201
Основная группа объекта	151	Пример 9: Применение списка прав доступа	202
Пользовательский профайл владельца по умолчанию (QDFTOWN)	152	Пример 10: Применение нескольких групп	203
Присвоение прав доступа и владельца для новых объектов	152	Пример 11: Сочетание различных типов прав доступа	204
Объекты, принимающие права доступа владельца	156	Кэш прав доступа	207
Принятые права доступа: риски и рекомендации	159		
Программы, игнорирующие принятые права доступа	160	Глава 6. Защита управления заданиями	209
Владельцы прав доступа	160	Инициализация задания	209
Владельцы прав доступа и перенос данных System/36	161	Запуск интерактивного задания	209
Риски при работе с владельцами прав доступа	162	Запуск пакетного задания	210
Работа с правами доступа	162	Принятые права доступа и пакетные задания	211
Меню прав доступа	162	Рабочие станции	211
Отчеты о правах доступа	164	Принадлежность описаний устройств	213
Работа с библиотеками	165	Файл меню входа в систему	214
Создание объектов	166	Изменение меню входа в систему	214
Работа с правами доступа к отдельным объектам	167	Исходный код меню входа в систему	214
Настройка пользовательских прав доступа	167	Изменение файла меню входа в систему	215
Предоставление прав доступа новым пользователям	168	Описания подсистем	215
Аннулирование прав доступа пользователя	168	Управление передачей новых заданий в систему	216
Работа с правами доступа к нескольким объектам	169	Описания заданий	216
Работа с принадлежностью объекта	171	Очередь сообщений системного оператора	217
Работа с правами доступа основной группы	172	Списки библиотек	218
Работа с модельным объектом	173	Риски, связанные с применением списков библиотек	218
Копирование прав доступа пользователя	173	Изменения в функции	219
Работа с списками прав доступа	173		
Преимущества списка прав доступа	174		
Создание списка прав доступа	174		
Предоставлению пользователям доступа к списку прав доступа	175		

Несанкционированный доступ к информации	219
Рекомендации по настройке системной части списка библиотек	219
Рекомендации по настройке рабочей библиотеки	220
Рекомендации по настройке текущей библиотеки	220
Рекомендации по настройке пользовательской части списка библиотек	221
Печать	221
Защита буферных файлов	222
Параметр очереди вывода Показать данные (DSPDATA)	222
Параметр очереди вывода Права на исправление (AUTCHK)	223
Параметр очереди вывода Управляется оператором (OPRCTL)	223
Параметры очереди вывода и права доступа, необходимые для печати	223
Примеры: очередь вывода	224
Атрибуты сети	225
Сетевой атрибут Действие над заданием (JOBACN)	225
Сетевой атрибут Обработка запросов клиентов (PCSACC)	226
Возможные риски и рекомендации	226
Сетевой атрибут Обработка запросов DDM (DDMACC)	227
Операции сохранения и восстановления	227
Ограничение доступа к командам сохранения и восстановления	228
Пример: ограничение доступа к командам сохранения и восстановления	228
Настройка производительности	229
Выполнение заданий только в пакетном режиме	229

Глава 7. Разработка схем защиты 231

Общие рекомендации по проектированию защиты	232
Планирование изменения уровня пароля	233
Изменение значения QPWLVL с 0 на 1	233
Изменение значения QPWLVL с 0 или 1 на 2	233
Изменение значения QPWLVL с 2 на 3	235
Переход с уровня QPWLVL на более низкий уровень пароля	235
Планирование библиотек	236
Планирование приложений, позволяющее избежать создания профайлов больших размеров	237
Списки библиотек	238
Управление списком пользовательских библиотек	238
Изменение списка системных библиотек	239
Сведения для защиты библиотек	240
Планирование меню	240
Сведения для защиты меню	241
Применение принятых прав доступа при разработке меню	242
Игнорирование принятых прав доступа	245
Системный запрос, меню	246
Планирование защиты команд	247
Планирование защиты файлов	248
Защита логических файлов	248
Переопределение файлов	251
Защита файлов и SQL	251

Планирование профайлов групп	251
Замечания об основной группе объектов	252
Особенности профайлов нескольких групп	252
Накопление специальных прав доступа для участников профайла группы	253
Применение профайла пользователя в качестве профайла группы	253
Сравнение профайлов групп и списков прав доступа	253
Планирование защиты от программистов	254
Управление исходными файлами	255
Защита файлов class и jar Java в интегрированной файловой системе	255
Планирование защиты от системных программистов и менеджеров	256
Работа с контрольными списками	256
Ограничение доступа к функциям программ	257

Глава 8. Резервное копирование и восстановление информации защиты 259

Хранение информации о защите	260
Сохранение информации о защите	261
Восстановление информации о защите	262
Восстановление пользовательских профайлов	262
Восстановление объектов	263
Восстановление прав доступа	266
Восстановление программ	266
Восстановление лицензионных программ	267
Восстановление списков прав доступа	268
Восстановление списка прав доступа со списком прав доступа	269
Восстановление операционной системы	269
Специальные права доступа *SAVSYS	270
Контроль операций сохранения и восстановления	270

Глава 9. Контроль эффективности защиты системы System i 271

Справочная таблица для системных администраторов и администраторов контроля	271
Физическая защита	272
Системные значения	272
Пользовательские профайлы, поставляемые IBM	272
Контроль паролей	273
Профайлы пользователей и групп	274
Управление доступом	275
Несанкционированный доступ	276
Несанкционированный доступ к программам	277
Средства связи	277
Работа с журналом контроля за действиями	277
Планирование контроля за действиями	278
Планирование контроля действий	278
Значения уровня контроля действий	279
Записи журнала контроля за действиями	285
Планирование контроля доступа к объектам	304
Показ контроля объектов	306
Настройка параметров контроля по умолчанию для объекта	306
Предотвращение потерь данных контроля	306
Выключение контроля объектов QTEMP	307

Настройка контроля за действиями с помощью CHGSECAUD	308
Настройка контроля за действиями	308
Управление журналом контроля и получателями журнала	310
Сохранение и удаление получателей журналов контроля	311
Получатели журнала, управляемые системой	312
Получатели журналов, управляемые пользователями	312
Выключение функции контроля	313
Анализ записей журнала контроля	313
Просмотр записей журнала контроля	313
Анализ записей журнала контроля с помощью утилиты запроса или программы	315
Сравнительное описание поля Дата и время изменения объекта и записей контроля	316
Другие способы контроля эффективности защиты системы	317
Отслеживание сообщений о попытках нарушения защиты	317
Работа с протоколом хронологии	318
Применение журналов для отслеживания операций с объектами.	318
Анализ пользовательских профайлов.	320
Печать выбранных пользовательских профайлов	320
Просмотр больших пользовательских профайлов	321
Анализ прав доступа к объектам и библиотекам	321
Анализ программ, принимающих права доступа	322
Проверка измененных объектов	322
Проверка операционной системы	323
Контроль действий системного администратора	323

Приложение А. Команды для организации защиты 327

Команды для работы с владельцами прав доступа	327
Команды для работы со списками прав доступа	327
Команды прав доступа к объектам и контроля	328
Команды для работы с паролями	329
Команды пользовательского профайла	330
Команды для работы с пользовательским профайлом	331
Команда контроля.	331
Команды для работы с объектами библиотеки документов	332
Команды для работы с записью идентификации сервера	332
Команды для работы с системным каталогом рассылки	333
Команды для работы с контрольными списками	333
Команды для работы с информацией об использовании функций	333
Команды для работы с инструментами защиты контроля	334
Команды для работы с инструментами защиты прав доступа	334
Команды для работы с инструментами защиты системы	335

Приложение В. Пользовательские профайлы, поставляемые IBM 337

Значения по умолчанию для пользовательских профайлов	337
Пользовательские профайлы, поставляемые IBM	339

Приложение С. Команды, поставляемые с общими правами доступа *EXCLUDE. 347

Приложение D. Права доступа, требуемые для объектов, используемых командами 359

Подразумеваемые права доступа, необходимые для выполнения команд	361
Общие правила относительно прав доступа к объектам, необходимых для выполнения команд	361
Общие команды для большинства объектов	364
Команды восстановления путей доступа.	371
Команды Advanced Function Presentation (AFP)	372
Команды для работы с сокетами AF_INET для SNA	373
Команды предупреждений	373
команды для разработки приложений	374
Команды для работы с владельцами прав доступа	375
Команды списка прав доступа	375
Команды для работы с каталогами связывания	376
Команды для работы с описанием запроса на изменение	376
Команды для работы с диаграммами	377
Команды для работы с классами	377
Команды для работы с классом обслуживания	378
Команды для работы с кластерами	378
Команды для работы с командами (*CMD).	382
Команды управления фиксацией	383
Команды исходной информации связи	383
Команды настройки	384
Команды списка конфигураций	385
Команды списка соединений	385
Команды для работы с описанием контроллера	386
Команды шифрования	388
Команды для работы с областью данных	389
Команды для работы с очередью данных	389
Команды для работы с описанием устройств	390
Команды для работы с эмуляцией устройств	392
Команды для работы с каталогами и теневыми каталогами	393
Команды для работы с сервером каталогов	393
Команды для работы с дисками	394
Команды для удаленного входа в систему дисплейной станции	394
Команды рассылки	395
Команды для работы с списком рассылки	396
Команды для работы с объектом библиотеки документов	396
Команды для работы с DNS	401
Команды для двухбайтовых кодировок	402
Команды описания формата	403
Команды для работы с переменными среды	403

Команды настройки расширенной беспроводной локальной сети	403	Команды для работы с программами	490
Команды для работы с файлами	404	Команды интерпретатора оболочки QSH	493
Команды для работы с фильтром	411	Команды для работы с запросами.	494
Финансовые команды.	412	Команды для работы с вопросами и ответами.	495
Команды для графических операций i5/OS	412	Команды для работы с программой чтения.	496
Команды для работы с набором графических символов	413	Команды средства регистрации	496
Команды для сервера хоста	413	Команды для работы с реляционной базой данных	497
Команды для работы с каталогом образов	413	Команды для работы с ресурсами	497
Команды интегрированной файловой системы	415	Команды для работы с записью удаленного задания (RJE)	497
Команды интерактивного определения данных	435	Команды для работы с атрибутами защиты	502
Команды для работы с Internetwork Packet Exchange (IPX)	436	Команды для работы с записью идентификации сервера	502
Команды для работы с индексом поиска	436	Служебные команды	502
Команды для работы с атрибутами IPL	436	Команды для работы с орфографическим словарем	507
Команды Java	437	Команды для работы с сферой управления	507
Команды для работы с заданиями	437	Команды буферного файла	508
Команды описания заданий	441	Команды для работы с описанием подсистемы	510
Команды очереди заданий	441	Системные команды	512
Команды расписания заданий	442	Команды системного списка ответов	513
Команды работы с журналами	443	Команды для работы с системными значениями	513
Команды для работы с получателем журнала	447	Команды среды System/36	513
Команды для работы с Kerberos	448	Команды для работы с таблицами	516
Команды для работы с языками программирования	450	Команды TCP/IP	516
Команды для работы с библиотеками	456	Команды описания часового пояса	517
Команды для работы с ключами лицензий	461	Команды для работы с информацией о заказе на обновление	518
Команды лицензионных программ	461	Команды для работы с пользовательским индексом, пользовательской очередью и пользовательским пространством	518
Команды описания линии	462	Команды для работы с пользовательской файловой системой	518
Команды для работы в локальной сети (LAN)	464	Команды для работы с пользовательским профайлом	520
Команды работы с локалью	464	Команды для работы с контрольным списком.	523
Команды среды почтового сервера	464	Команды настройки рабочей станции	523
Команды для работы с носителями	464	Команды для работы с загрузчиками.	523
Команды для работы с группами панелей и меню	465		
Команды для работы с сообщениями	466		
Команды для работы с описанием сообщений	467		
Команды для работы с файлами сообщений	468		
Команды для работы с очередью сообщений	468		
Команды переноса данных	468		
Команды описания режима	469		
Команды для работы с модулями	469		
Команды описания NetBIOS	470		
Команды для работы с сетью	471		
Команды для работы с сетевой файловой системой	472		
Команды для работы с описанием сетевого интерфейса	473		
Команды для работы с сетевым сервером	473		
Команды настройки сетевого сервера	474		
Команды для работы с описанием сетевого сервера	475		
Команды для работы со списком узлов	475		
Команды служб Office	476		
Команды диалогового обучения	476		
Команды операционной поддержки	477		
Команды для работы с оптической памятью	478		
Команды очереди вывода	480		
Команды для работы с пакетами	482		
Команды для работы со статистикой.	482		
Команды для работы с группой дескрипторов печати	488		
Команды настройки Print Services Facility	489		
Команды для работы с неполадками	489		
		Приложение Е. Работа с объектами и контроль за объектами	527
		Общие операции для всех типов объектов	527
		Операции над временем восстановления путей доступа	530
		Операции над таблицей предупреждений (*ALRTBL)	531
		Операции над списком прав доступа (*AUTL)	531
		Операции над владельцем прав доступа (*AUTHLR)	532
		Операции над каталогом связывания (*BNDDIR)	532
		Операции над списком конфигурации (*CFGL).	533
		Операции над специальными файлами (*CHRSE)	533
		Операции над форматом диаграммы (*CHTFMT)	533
		Операции над описанием локали C (*CLD)	534
		Операции с описанием запроса на изменение (*CRQD)	534
		Операции над классами (*CLS).	535
		Операции над командами (*CMD).	535
		Операции над списком соединений (*CNL)	536
		Операции над описанием класса обслуживания (*COSD)	537
		Операции над исходной информацией связи (*CSI)	537
		Операции над списком межсистемных продуктов (*CSPMAP)	537

Операции над таблицей межсистемных продуктов (*CSPTBL)	538
Операции над описанием контроллера (*CTLD)	538
Операции над описанием устройства (*DEVDD)	539
Операции над каталогом (*DIR)	540
Операции с сервером каталогов	542
Операции над объектом библиотеки документов (*DOC или *FLR)	544
Операции над областью данных (*DTAARA)	547
Операции в Утилите интерактивного определения данных (*DTADCT)	548
Операции над очередью данных (*DTAQ)	548
Операции над описанием формата (*EDTD)	549
Операции над записями регистрации точек выхода (*EXITRG)	549
Операции над таблицей управления формами (*FCT)	550
Операции над файлами (*FILE)	550
Операции над файлами FIFO (*FIFO)	553
Операции над папкой (*FLR)	554
Операции над ресурсом шрифта (*FNTRSC)	554
Операции над определением формы (*FORMDF)	554
Операции над объектом фильтра (*FTR)	554
Операции над набором графических символов (*GSS)	555
Операции над словарем набора двухбайтовых символов (*IGCDCT)	556
Операции над сортировкой набора двухбайтовых символов (*IGCSRT)	556
Операции над таблицей набора двухбайтовых символов (*IGCTBL)	556
Операции над описанием задания (*JOBDD)	557
Операции над очередью заданий (*JOBQ)	557
Операции над планировщиком заданий (*JOBSCD)	558
Операции над журналом (*JRN)	559
Операции над получателем журнала (*JRNRCV)	560
Операции над библиотекой (*LIB)	561
Операции над описанием линии (*LIND)	561
Операции над почтовыми службами	562
Операции над меню (*MENU)	563
Операции над описанием режима (*MODD)	563
Операции над объектом модуля (*MODULE)	564
Операции над файлом сообщений (*MSGF)	564
Операции над очередью сообщений (*MSGQ)	565
Операции над группой узлов (*NODGRP)	566
Операции над списком узлов (*NODL)	566
Операции над описанием NetBIOS (*NTBD)	567
Операции над сетевым интерфейсом (*NWID)	567
Операции над описанием сетевого сервера (*NWSD)	568
Операции над очередью вывода (*OUTQ)	568
Операции над перекрытием (*OVL)	570
Операции над определением страницы (*PAGDFN)	570
Операции над сегментом страницы (*PAGSEG)	570
Операции над группой дескрипторов печати (*PDG)	571
Операции над программой (*PGM)	571
Операции над группой панелей (*PNLGRP)	572
Операции над уровнем готовности продукта (*PRDAVL)	573
Операции над определением продукта (*PRDDFN)	573
Операции над компоновкой программных продуктов (*PRDLOD)	573
Операции над формой Query Manager (*QMFORM)	573
Операции над запросом Query Manager (*QMQR)	574
Операции над определением запроса (*QRYDFN)	575
Операции над таблицей преобразования информационных кодов (*RCT)	576
Операции над списком ответов	576
Операции над описанием подсистемы (*SBSD)	577
Операции над индексом поиска информации (*SCHIDX)	578
Операции над локальным сокетом (*SOCKET)	578
Операции над орфографическим словарем (*SPADCT)	580
Операции над буферными файлами	581
Операции над пакетом SQL (*SQLPKG)	582
Операции над служебной программой (*SRVPGM)	583
Операции над описанием сеанса (*SSND)	584
Операции над областью памяти сервера (*SVRSTG)	584
Операции над потоковым файлом (*STMF)	584
Операции над символьными ссылками (*SYMLNK)	586
Операции над описанием системы S/36 (*S36)	587
Операции над таблицей (*TBL)	588
Операции над пользовательским индексом (*USRIDX)	588
Операции над пользовательским профайлом (*USRPRF)	589
Операции над пользовательской очередью (*USRQ)	590
Операции над пользовательским пространством (*USRSPC)	590
Операции над контрольным списком (*VLDL)	590
Операции над объектом настройки рабочей станции (*WSCST)	591

Приложение F. Макет записей журнала контроля 593

Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)	594
Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)	596
Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)	597
Типы записей журнала контроля (QAUDJRN)	598
Записи журнала AD (изменение параметров контроля)	600
Записи журнала AF (ошибка прав доступа)	604
Записи журнала AP (Принятые права доступа)	611
Записи журнала AU (изменение атрибутов)	611
Записи журнала CA (изменение прав доступа)	612
Записи журнала CD (командная строка)	615
Записи журнала CO (создание объекта)	616
Записи журнала CP (изменение пользовательского профайла)	618
Записи журнала CQ (изменение *CRQD)	621
Записи журнала CU (операции с кластерами)	622
Записи журнала CV (проверка соединения)	624
Записи журнала CY (настройка шифрования)	626
Записи журнала DI (сервер каталогов)	628
Записи журнала DO (операция удаления)	635
Записи журнала DS (сброс поставляемого IBM ИД пользователя сервисных средств)	637
Записи журнала EV (переменная среды)	638
Записи журнала GR (шаблон записи)	639
Записи журнала GS (предоставить дескриптор)	644

Записи журнала IM (монитор вторжений)	644
Записи журнала IP (обмен данными между процессами)	648
Записи журнала IR (действия правил обработки пакетов IP)	649
Записи журнала IS (управление защитой в Internet)	651
Записи журнала JD (изменение описания задания)	653
Записи журнала JS (изменение задания)	654
Записи журнала KF (файл набора ключей)	659
Записи журнала LD (создание и удаление ссылок, поиск в каталоге)	662
Записи журнала ML (действия с почтой)	664
Записи журнала NA (изменение атрибута)	664
Записи журнала ND (фильтр поиска в каталоге APPN)	665
Записи журнала NE (фильтр конечной точки APPN)	666
Записи журнала OM (изменение параметров управления объектами)	667
Записи журнала OR (восстановление объекта)	670
Записи журнала OW (изменение владельца)	674
Записи журнала O1 (доступ к оптической памяти)	676
Записи журнала O2 (доступ к оптической памяти)	677
Записи журнала O3 (доступ к оптической памяти)	679
Записи журнала PA (принятие прав доступа программой)	680
Записи журнала PG (изменение основной группы)	682
Записи журнала PO (вывод на принтер)	685
Записи журнала PS (смена профайла)	687
Записи журнала PW (пароль)	689
Записи журнала RA (изменение прав доступа восстановленного объекта)	690
Записи журнала RJ (восстановление описания задания)	692
Записи журнала RO (изменение владельца восстановленного объекта)	693
Записи журнала RP (восстановление программ, принимающих права доступа)	695
Записи журнала RQ (восстановление дескриптора запроса на изменение)	697
Записи журнала RU (восстановить права доступа пользовательского профайла)	697
Записи журнала RZ (изменение основной группы восстановленного объекта)	698
Записи журнала SD (изменить системный каталог рассылки)	700
Записи журнала SE (изменение записи о выполнении подсистемы)	701
Записи журнала SF (действие над буферным файлом)	702
Записи журнала SG (асинхронные сигналы)	707
Записи журнала SK (соединения SSL)	708
Записи журнала SM (изменение параметров управления системами)	710
Записи журнала SO (действия над пользовательской информацией о защите сервера)	711

Записи журнала ST (обращение к сервисным средствам)	712
Записи журнала SV (действие над системным значением)	717
Записи журнала VA (изменение списка управления доступом)	719
Записи журнала VC (запуск и завершение соединения)	719
Записи журнала VF (заккрытие файлов сервера)	720
Записи журнала VL (превышено ограничение для учетной записи)	721
Записи журнала VN (вход в сеть и выход из нее)	722
Записи журнала VO (контрольный список)	723
Записи журнала VP (ошибка в сетевом пароле)	725
Записи журнала VR (обращение к сетевому ресурсу)	725
Записи журнала VS (сеанс сервера)	726
Записи журнала VU (изменение сетевого профайла)	727
Записи журнала VV (изменение состояния службы)	728
Записи журнала X0 (сетевая идентификация)	729
Записи журнала X1 (идентификационный маркер)	734
Записи журнала XD (расширение сервера каталогов)	737
Записи журнала YC (изменение объекта DLO)	738
Записи журнала YR (чтение объекта DLO)	739
Записи журнала ZC (изменение объекта)	740
Записи журнала ZR (чтение объекта)	743
Коды типов доступа	745

Приложение G. Команды и меню защиты	749
Опции меню Инструменты защиты	749
Применение меню защиты в пакетном режиме	752
Опции меню SECWATCH	754
Команды для тонкой настройки защиты	758
Значения, устанавливаемые командой Настроить защиту системы	759
Изменение программы	761
Команда Аннулировать общие права доступа	761
Изменение программы	762

Приложение H. Связанная информация для справочника по защите i5/OS	765
---	------------

Приложение I. Примечания	769
Сведения о программных интерфейсах	771
Товарные знаки	771
Условия и соглашения	771

Индекс	773
-------------------------	------------

Новое в V6R1

Здесь приведена информация о новых разделах справочника по защите.

Новые системные значения

Блокировка изменения пароля (QPWDCHGBLK)

Системное значение Блокировка изменения пароля (QPWDCHGBLK) задает время, в течение которого запрещено изменение пароля после предыдущего изменения.

Предупреждение об истечении срока действия пароля (QPWDEXPWRN)

Системное значение Предупреждение об истечении срока действия пароля (QPWDEXPWRN) задает число дней, оставшихся до устаревания пароля, когда при входе в систему пользователю показывается предупреждение об истечении срока действия пароля.

Правила паролей (QPWDRULES)

Системное значение Правила паролей (QPWDRULES) задает правила, применяемые для проверки правильности паролей. В системном значении QPWDRULES можно указать несколько значений, если не указано значение *PWDSYSVAL.

Список шифров Secure Sockets Layer (SSL) (QSSLCSL)

Системное значение Список шифров Secure Sockets Layer (SSL) (QSSLCSL) указывает, какие шифры поддерживаются системными функциями SSL.

Управление шифрами Secure Sockets Layer (SSL) (QSSLCSLCTL)



Системное значение Управление шифрами Secure Sockets Layer (SSL) (QSSLCSLCTL) указывает, кто управляет системным значением Список шифров Secure Sockets Layer (SSL) (QSSLCSL), система или пользователь.

Протоколы Secure Sockets Layer (SSL) (QSSLPCL)

Системное значение Протоколы Secure Sockets Layer (SSL) (QSSLPCL) указывает, какие протоколы SSL поддерживаются системными функциями.

Как просмотреть новые и измененные функции выпуска

Для упрощения поиска изменений в Information Center используются такие значки:

- Значок  отмечает начало новой или измененной информации.
- Значок  отмечает конец новой или измененной информации.

В файлах PDF новая и измененная информация выделена в левом поле символом (|).

Глава 1. Введение в защиту System i

Семейство IBM Systems спроектировано для широкого круга пользователей. В системе System i предусмотрены достаточно гибкие средства защиты, способные удовлетворить требованиям широкого круга пользователей в самых различных ситуациях.

В небольшой системе может быть зарегистрировано от трех до пяти пользователей, в большой - до нескольких тысяч пользователей. В некоторых случаях все рабочие станции расположены в отдельном помещении, как правило, недоступном посторонним лицам. В других случаях пользователи могут быть разбросаны по всему миру и могут подключаться, например, удаленно или, в качестве косвенных пользователей, через персональные компьютеры и сети. Вы должны изучить основные средства, функции и опции защиты, чтобы приспособить их к выбранной конфигурации.

Защита системы преследует три основные цели:

Конфиденциальность:

- Защита от несанкционированного доступа к информации
- Ограничение доступа к конфиденциальной информации
- Защита от прочих пользователей системы и посторонних лиц

Целостность:

- Защита данных от несанкционированного изменения
- Предоставление доступа к данным только уполномоченным программам
- Обеспечение достоверности данных

Доступность:

- Предотвращение случайного изменения и повреждения данных
- Защита от неправильного обращения с данными и уничтожения данных посторонними лицами

Зачастую под защитой системы понимают прежде всего меры по противодействию внешним угрозам, таким как действия хакеров и конкурентов по бизнесу. Однако, как правило, наиболее важным преимуществом правильно построенной защиты является защита от случайных действий пользователей. Если система хорошо защищена от атак извне, но не защищена от случайных действий пользователей, то нажатие неверной клавиши может привести к удалению важной информации. Правильное построение защиты позволяет предотвратить случайности такого типа.

Без тщательного планирования даже самые лучшие функции защиты не позволят достичь хороших результатов. Защита, собранная из отдельных фрагментов, не связанных единым планом, может лишь затруднить работу в системе. Такую защиту трудно обслуживать и контролировать. Планирование отнюдь не подразумевает разработку защиты для каждого файла, программы или устройства. Планирование предполагает разработку общих принципов организации защиты системы и ознакомление с этими принципами всех разработчиков приложений, программистов и пользователей системы.

При планировании защиты системы и принятии решения об уровне защиты ответьте на следующие вопросы:

- Существует ли в компании стратегия или стандарт, предусматривающие определенный уровень защиты?
- Необходим ли определенный уровень защиты аудиторам компании?
- Насколько важны система и хранящиеся в ней данные для вашего бизнеса?
- Насколько важна защита от ошибок, предоставляемая функциями защиты?
- Какие требования к защите предъявляются вашей компанией на будущее?

Для упрощения установки многие функции защиты отключены на момент поставки системы. В этих разделах приведены рекомендации, позволяющие создать приемлемый уровень защиты системы. Проанализируйте эти рекомендации с учетом предъявляемых требований к защите.

Физическая защита

Физическая защита предусматривает защиту системного блока, системных устройств и резервных носителей от случайного или преднамеренного повреждения. Большинство мер по обеспечению физической защиты системы носят внешний характер по отношению к самой системе. Однако система оснащена электронным или обычным ключом, позволяющим ограничить доступ к функциям системного блока.

Примечание: Для некоторых моделей ключ заказывается дополнительно.

Информация, связанная с данной

Планирование физической защиты

Защита с помощью ключа

Получить или изменить позицию ключа можно с помощью API. Получить атрибуты IPL (QWCRIPLA) или команды Изменить атрибуты IPL (CHGIPLA).

Ключ, расположенный на панели управления 940х, позволяет ограничить доступ к различным функциям системной панели управления.

Функции ключа позволяют удаленным пользователям работать с дополнительными функциями, предусмотренными в панели управления. Например, с панели управления можно выбирать источник IPL системы и загружаемую среду: i5/OS или Специальные сервисные средства (DST).

Системное значение QRMTSRVATR i5/OS позволяет управлять удаленным доступом. По умолчанию во время поставки это значение не применяется, так что положение ключа изменить невозможно. Для того чтобы разрешить удаленный доступ, измените это системное значение. Учтите, что для этого требуются специальные права доступа *SECADM и *ALLOBJ.

Ссылки, связанные с данной

“Атрибут удаленного обслуживания (QRMTSRVATR)” на стр. 42

Атрибут удаленного обслуживания (QRMTSRVATR) позволяет управлять функциями анализа неполадок удаленного обслуживания. С помощью этого значения можно выполнить удаленный анализ системы.

Уровень защиты

Платформа System i поддерживает пять уровней защиты. С помощью системного значения Уровень защиты (QSECURITY) вы можете задать уровень защиты системы.

Уровень 10:

Уровень 10 больше не поддерживается.

Уровень 20:

Для входа в систему требуется указать ИД пользователя и пароль. Всем пользователям предоставляются права доступа ко всем объектам.

Уровень 30:

Для входа в систему требуется указать ИД пользователя и пароль. Применяется защита ресурсов.

Уровень 40:

Для входа в систему требуется указать ИД пользователя и пароль. Применяется защита ресурсов. Кроме того, применяются функции защиты целостности.

Уровень 50:

Для входа в систему требуется указать ИД пользователя и пароль. Применяется защита ресурсов.

Применяются функции защиты целостности уровня 40 и расширенные функции защиты целостности. Уровень 50 удовлетворяет требованиям к защите Common Criteria (CC) и предназначен для систем System i с высокими требованиями к защите.

Ссылки, связанные с данной

Глава 2, “Работа с системным значением Защита системы (QSecurity)”, на стр. 9

С помощью системного значения Уровень защиты (QSECURITY) вы можете задать степень защищенности системы.

Системные значения

Системные значения позволяют настроить многие параметры платформы System i. Системные значения можно использовать для указания глобальных параметров защиты.

Например, вы можете указать следующее:

- Число разрешенных попыток входа в систему.
- Необходимость отключения неактивной рабочей станции.
- Частоту смены паролей.
- Длину и состав паролей.

Понятия, связанные с данным

Глава 3, “Системные значения защиты”, на стр. 25

Системные значения позволяют настроить различные характеристики системы. Для определения общесистемных параметров защиты предусмотрена группа системных значений.

Цифровые подписи

Цифровые подписи позволяют усилить защиту программных объектов.

Ключевым компонентом защиты является *целостность*: защита от несанкционированного изменения и повреждения объектов. Программное обеспечение операционной системы System i защищено цифровыми подписями.

Гарантия подлинности приобретает особое значение, когда объект передается по сети Internet или хранится на общедоступных носителях. Электронная подпись позволяет определить, был ли изменен объект в процессе передачи.

Цифровыми подписями и способами их применения для проверки целостности программного обеспечения можно управлять в соответствии со стратегиями защиты: с помощью системного значения Проверять восстанавливаемые объекты (QVIFYOBJRST), команды Проверить целостность объекта (CHKOBJTG) и программы Диспетчер цифровых сертификатов (DCM). Кроме того, вы можете подписывать собственные программы (все лицензионные программы, поставляемые с системой, подписаны).

Можно запретить добавление цифровых сертификатов в хранилище сертификатов с помощью нового API Добавить программу проверки, а также запретить сброс паролей хранилища цифровых сертификатов. В Системный инструментарий (SST) добавлена новая опция меню “Работа с защитой системы”, позволяющая запретить добавление цифровых сертификатов.

Информация, связанная с данной

Применение цифровых подписей для защиты целостности программ

Диспетчер цифровых сертификатов

Включение единого входа в систему

Единый вход в систему - это способ идентификации, при котором пользователь использует один ИД и пароль для входа в несколько систем. В современных неоднородных сетях, содержащих серверы, разбитые на логические разделы, и системы с разными платформами, управление идентификацией пользователей сети становится все более трудной задачей.

Для обеспечения среды единого входа в систему IBM предоставляет две технологии, совместное применение которых позволяет пользователям, зарегистрировавшимся в Windows со своими именем и паролем автоматически получать доступ к системам System i в сети. Для реализации среды единого входа в систему администратор должен настроить Службу сетевой идентификации (NAS) и Преобразование идентификаторов в рамках предприятия (EIM). В операционных системах Windows 2000, Windows XP, AIX и z/OS идентификация пользователей выполняется на основе протокола Kerberos. Идентификацию субъектов (пользователей Kerberos) в сети выполняет защищенная централизованная система, называемая Центром распределения ключей.

Служба сетевой идентификации позволяет добавить систему System i в область Kerberos, а технология EIM обеспечивает механизм связывания субъекта Kerberos с единым идентификатором EIM, представляющим пользователя в пределах всего предприятия. С идентификатором EIM можно связать и другие идентификаторы пользователя, например имя пользователя i5/OS. После того как пользователь зарегистрировался в сети, для входа в систему System i ему не нужно повторно вводить имя пользователя и пароль. Если идентификация Kerberos выполнена успешно, приложения могут найти имя пользователя i5/OS по идентификатору EIM. При этом пользователю не требуется вводить пароль для работы с приложениями и функциями System i, так как его идентификация уже выполнена с помощью протокола Kerberos. Администраторам предоставляется возможность централизованно управлять пользовательскими профайлами, а пользователям сети достаточно запомнить один пароль. Настроив в системе службу сетевой идентификации (NAS) и технологию преобразования идентификаторов в рамках предприятия (EIM), вы можете применить среду единого входа в систему.

Информация, связанная с данной

Сценарий: создание тестовой среды единого входа в систему

Пользовательские профайлы

У каждого пользователя в системе i5/OS есть пользовательский профайл.

На уровне защиты 10 система автоматически создает пользовательский профайл при первом входе пользователя в систему. На более высоких уровнях защиты пользовательские профайлы создаются администратором - только после этого пользователь сможет войти в систему.

Пользовательский профайл - это мощный и гибкий инструмент. В нем определяются возможности пользователя по работе в системе. Ниже приведено описание нескольких важных функций пользовательских профайлов, связанных с защитой:

Специальные права доступа

Специальные права доступа позволяют пользователю выполнять системные функции, например создавать пользовательские профайлы и изменять задания других пользователей.

Начальное меню и начальная программа

Начальное меню и начальная программа определяют набор функций, доступных для пользователя после входа в систему. С помощью начального меню вы можете ограничить возможности пользователя заданным набором задач.

Ограничить возможности

Поле пользовательского профайла Ограничить возможности позволяет определить, может ли пользователь вводить команды и изменять начальное меню и начальную программу при входе в систему.

Понятия, связанные с данным

Глава 4, “Пользовательские профайлы”, на стр. 77

Пользовательские профайлы - это мощный и гибкий инструмент. Правильная организация пользовательских профайлов поможет защитить систему и настроить ее для пользователей.

Профайлы групп

Профайл группы - это особый тип пользовательского профайла. Если требуется предоставить одинаковые права доступа нескольким пользователям, то с помощью профайла группы вы можете сделать это за один прием.

Профайлу группы могут принадлежать объекты системы. Кроме того, профайл группы можно применять в качестве шаблона для создания отдельных пользовательских профайлов. Для этой цели предусмотрена функция копирования профайла.

Понятия, связанные с данным

“Планирование профайлов групп” на стр. 251

Профайл группы - это эффективный инструмент для управления несколькими профайлами пользователей с одинаковыми требованиями к защите. Можно либо специально создать профайл группы, либо преобразовать в профайл группы один из существующих профайлов. Профайлы групп позволяют повысить эффективность управления правами доступа и сократить число записей о частных правах доступа к отдельным объектам.

“Групповая принадлежность объектов” на стр. 150

В этом разделе описаны особенности принадлежности объектов к группе.

“Основная группа объекта” на стр. 151

Для объекта можно задать основную группу.

“Копирование пользовательского профайла” на стр. 124

Пользовательский профайл можно создать путем копирования другого пользовательского профайла или профайла группы.

Защита ресурсов

Разрешение на работу с объектом называется *правами доступа*. Защита ресурсов в операционной системе i5/OS позволяет настроить права доступа к объектам и указать, кому и как будет разрешено работать с объектами.

Вы можете указать уточненные права доступа, такие как возможность добавления или изменения записей. Кроме того, предусмотрены системные подмножества прав доступа: *ALL, *CHANGE, *USE и *EXCLUDE.

Чаще всего защиту ресурсов устанавливают для файлов, программ и библиотек, но права доступа можно определить для любого объекта системы. Ниже перечислены функции защиты ресурсов:

Профайлы групп

Группа пользователей, обладающих одинаковыми правами доступа к объектам.

Списки прав доступа

Объекты, для которых необходим одинаковый уровень защиты, могут быть объединены в одну группу. В этом случае права доступа можно указать сразу для всего списка, а не для каждого объекта в отдельности.

Принадлежность объекта

У любого объекта системы есть владелец. Объекты могут принадлежать как отдельному пользовательскому профайлу, так и профайлу группы. Правильное распределение объектов по владельцам упрощает управление приложениями и распределение ответственности за защиту информации.

Основная группа

Для объекта можно задать основную группу. Права доступа основной группы хранятся вместе с объектом. Применение основной группы позволяет упростить управление правами доступа и ускорить проверку прав доступа.

Права доступа к библиотеке

Файлы и программы с одинаковыми требованиями к защите можно поместить в библиотеку, доступ к которой ограничен. Как правило, такой подход более эффективен, чем ограничение доступа к каждому объекту по отдельности.

Права доступа к каталогу

Права доступа к каталогу применяются аналогично правам доступа к библиотеке. Вы можете сохранить объекты в каталоге, доступ к которому ограничен.

Права доступа к объекту

Если ограничение доступа с помощью библиотек и каталогов не позволяет получить достаточной точности, вы можете ограничить доступ к отдельным объектам.

Общие права доступа

Для каждого объекта можно указать права доступа, которые по умолчанию будут предоставляться всем пользователям системы, не имеющим каких-либо других прав доступа к этому объекту. Общие права доступа - это эффективное средство защиты информации, обеспечивающее высокую производительность.

Принятые права доступа

Принятые права доступа позволяют добавить к правам доступа пользователя, работающего с программой, права доступа пользователя, создавшего эту программу. Принятые права доступа удобны, когда требуется изменять права доступа пользователя в зависимости от обстоятельств.

Владелец прав доступа

Владелец прав доступа хранит информацию о правах доступа к файлу базы данных, описанному в программе. Информация о правах доступа сохраняется даже после удаления файла. Как правило, владельцы прав доступа применяются при переходе от System/36 к OS/400, так как приложения System/36 часто удаляют файлы и создают их заново.

Права доступа на уровне поля

Права доступа на уровне поля выделяются отдельным полям файла базы данных. Управлять этими правами доступа можно с помощью операторов SQL.

Понятия, связанные с данным

Глава 5, “Защита ресурсов”, на стр. 137

В этом разделе описаны все компоненты защиты ресурсов и приведена информация об их совместном применении для защиты информации в системе. Кроме того, здесь вы сможете найти сведения о настройке защиты ресурсов с помощью команд и меню CL.

Журнал контроля за действиями

Журнал контроля за действиями повышает эффективность защиты системы.

Операционная система i5/OS позволяет заносить записи о выбранных событиях, связанных с защитой, в журнал контроля за действиями. События для занесения в журнал задаются с помощью ряда системных значений, значений пользовательских профайлов и значений объектов.

Понятия, связанные с данным

Глава 9, “Контроль эффективности защиты системы System i”, на стр. 271

В этом разделе описаны возможные способы контроля эффективности защиты системы.

Среда защиты Common Criteria

Common Criteria - это среда для независимого анализа и тестирования соответствия продуктов требованиям защиты.

10 августа 2005 г. фирма IBM получила сертификат Common Criteria на операционную систему i5/OS V5R3M0 на уровне Evaluated Assurance Level (EAL) 4, дополненный ALC_FLR.2 для Controlled Access Protection Profile (CAPP), версия 1.d, от 8 октября 1999 г. Для того чтобы получить сертифицированную систему, закажите Common Criteria FC 1930 с номером 5722-SS1.

Этот компонент должны заказывать только те пользователи, которые должны работать в конфигурации Common Criteria.

Продукт помещен на страницу Validated Products List Web-сайта Common Criteria Evaluation and Validation Scheme.

Независимый пул дисков

Независимый пул дисков позволяет группировать память, которую можно подключать и отключать независимо от данных системы и других несвязанных данных. Термины *независимый ASP (iASP)* и *независимый пул дисков* являются синонимами.

Независимый пул дисков можно переносить между несколькими системами, входящими в состав кластера, либо подключить только к одной системе. Функциональные изменения, внесенные в независимые пулы дисков в V5R2, связаны с защитой системы. Например, при выполнении команды CRTUSRPRF нельзя создать пользовательский профайл (*USRPRF) в независимом пуле дисков. Однако, если пользователь обладает частными правами доступа к объекту из независимого пула дисков, является владельцем такого объекта или входит в состав основной группы этого объекта в независимом пуле дисков, то имя пользовательского профайла хранится в независимом пуле дисков. В случае перемещения независимого пула дисков в другую систему записи о частных правах доступа, принадлежности объектов и основных группах прикрепляются к пользовательскому профайлу с тем же именем в целевой системе. Если в целевой системе нет такого профайла, то он будет создан. При этом пользователю не предоставляются специальные права доступа, а в качестве пароля указывается значение *NONE.

Независимые пулы дисков поддерживают многие объекты библиотек и пользовательских файловых систем. Однако некоторые объекты запрещено размещать в независимых дисковых пулах. В i5/OS V5R1 независимые пулы дисков можно применять только с пользовательскими файловыми системами.

Информация, связанная с данной

Поддерживаемые и неподдерживаемые типы объектов

Глава 2. Работа с системным значением Защита системы (QSecurity)

С помощью системного значения Уровень защиты (QSECURITY) вы можете задать степень защищенности системы.

Описание

Задача:

Задаёт уровень защиты, применяемый в системе.

Средства для ее решения:

WRKSYSVAL *SEC (команда Работа с системными значениями) или меню Настройка, опция 1 (Изменить опции системы)

Права доступа:

*ALLOBJ и *SECADM

Запись в журнале:

SV

Прим.: Перед изменением этого значения в рабочей системе ознакомьтесь с соответствующей информацией о переходе с одного уровня защиты на другой.

Уровни защиты

Можно выбрать один из пяти уровней защиты:

10 Защита не применяется

Примечание: Уровень 10 нельзя указать с помощью системного значения QSECURITY.

20 Защита входа в систему

30 Защита входа в систему и ресурсов

40 Защита входа в систему, ресурсов и целостности

50 Защита входа в систему и ресурсов, расширенная защита целостности

Во время поставки система находится на уровне 40, который обеспечивает защиту входа в систему, ресурсов и целостности. Более подробная информация приведена в разделе “Уровень защиты 40” на стр. 14.

Для того чтобы изменить уровень защиты, выполните команду Работа с системными значениями (WRKSYSVAL). Следует применять защиту как минимум уровня 30. Однако рекомендуется уровень не ниже 40. Изменения вступают в силу после очередной загрузки начальной программы (IPL). В таблице Табл. 1 приведено сравнение уровней защиты системы:

Таблица 1. Уровни защиты: сравнение функций

Функция	Уровень 20	Уровень 30	Уровень 40	Уровень 50
Для входа в систему запрашивается имя пользователя	Да	Да	Да	Да
Для входа в систему запрашивается пароль	Да	Да	Да	Да
Защита паролем	Да	Да	Да	Да
Защита меню и начальной программы	Да ¹	Да ¹	Да ¹	Да ¹
Поддержка ограничения возможностей	Да	Да	Да	Да

Таблица 1. Уровни защиты: сравнение функций (продолжение)

Функция	Уровень 20	Уровень 30	Уровень 40	Уровень 50
Защита ресурсов	Нет	Да	Да	Да
Доступ ко всем объектам	Да	Нет	Нет	Нет
Автоматическое создание пользовательского профайла	Нет	Нет	Нет	Нет
Доступные функции контроля за действиями	Да	Да	Да	Да
Запрет на создание и повторную компиляцию программ, содержащих запрещенные команды	Да	Да	Да	Да
Запрет на выполнение программ, применяющих неподдерживаемые интерфейсы	Нет	Нет	Да	Да
Расширенная защиты аппаратной памяти включена для всех носителей.	Нет	Нет	Да	Да
Библиотека QTEMP применяется в качестве временного объекта	Нет	Нет	Нет	Нет
Объекты *USRSPC, *USRIDX и *USRQ можно создавать только в библиотеках, указанных в системном значении QALWUSRDMN	Да	Да	Да	Да
Проверка указателей в параметрах программ пользовательского домена, выполняющихся в режиме системы	Нет	Нет	Да	Да
Применение правил обработки сообщений, передаваемых между программами режима системы и режима пользователя	Нет	Нет	Нет	Да
Запрещено прямое изменение связанного пространства программы.	Нет	Нет	Да	Да
Защита внутренних управляющих блоков	Нет	Нет	Да	Да ²
¹ Если в пользовательском профайле указан параметр LMTCPB(*YES). ² На уровне 50 внутренние управляющие блоки дополнительно защищены по сравнению с уровнем 40. Информация приведена в разделе “Запрет на изменение внутренних управляющих блоков” на стр. 22.				

Специальные права доступа по умолчанию

В зависимости от уровня защиты системы, каждому классу пользователей по умолчанию предоставляются те или иные специальные права доступа. При создании пользовательского профайла вы можете выбрать специальные права доступа в соответствии с классом пользователя. Кроме того, специальные права доступа пользовательских профайлов добавляются или удаляются при изменении уровня защиты.

Для пользователя можно указать следующие специальные права доступа:

*ALLOBJ

Специальные права доступа ко всем объектам позволяют выполнять операции над всеми объектами.

*AUDIT

Специальные права на контроль позволяют определять параметры контроля за системой, объектами и пользователями системы.

*IOSYSCFG

Специальные права доступа к конфигурации системы позволяют настраивать устройства ввода-вывода в системе.

*JOBCTL

Специальные права на управление заданиями позволяют управлять пакетными заданиями и печатью.

*SAVSYS

Права на сохранение системы позволяют сохранять и восстанавливать объекты.

*SECADM

Специальные права администратора защиты позволяют работать с пользовательскими профайлами системы.

*SERVICE

Специальные служебные права доступа позволяют выполнять функции обслуживания программного обеспечения системы.

*SPLCTL

Специальные права на управление буфером предоставляют неограниченный контроль над пакетными заданиями и очередями вывода системы.

Вы можете запретить пользователям с правами доступа *SECADM и *ALLOBJ изменять командой CHGSYSVAL это системное значение, связанное с защитой. Для этого воспользуйтесь опцией "Работа с защитой системы" Системного инструментария (SST).

Примечание: Данное ограничение применимо и к некоторым другим системным значениям. Подробные сведения о том, как запретить изменение системных значений, а также полный список соответствующих системных значений приведены в разделе Системные значения защиты.

В таблице Табл. 2 перечислены специальные права доступа по умолчанию, предоставляемые всем классам пользователей. В записях может быть указано, что права доступа предоставляются только на уровнях 10 и 20, на всех уровнях защиты, либо не предоставляются.

Таблица 2. Специальные права доступа по умолчанию для класса пользователя на разных уровнях защиты

Специальные права	Классы пользователей				
	*SECOFR	*SECADM	*PGMR	*SYSOPR	*USER
*ALLOBJ	Все	10 или 20	10 или 20	10 или 20	10 или 20
*AUDIT	Все				
*IOSYSCFG	Все				
*JOBCTL	Все	10 или 20	10 или 20	Все	
*SAVSYS	Все	10 или 20	10 или 20	Все	10 или 20
*SECADM	Все	Все			
*SERVICE	Все				
*SPLCTL	Все				

Примечание: В разделах "Класс пользователя" на стр. 83 и "Специальные права доступа" на стр. 89 приведена дополнительная информация о классах пользователей и специальных правах доступа.

Замечания

Рекомендуется применять уровень защиты 30 или выше, так как на более низких уровнях система автоматически разрешает доступ ко всем ресурсам: всем пользователям предоставляются специальные права доступа *ALLOBJ.

Кроме того, на уровне защиты 30 (и ниже) пользователи могут вызывать системные интерфейсы, позволяющие работать от имени пользовательского профайла QSECOFR, а также работать с ресурсами, обычно им недоступными. На уровне защиты 40 пользователи не могут напрямую вызывать эти интерфейсы. По этой причине настоятельно рекомендуется применять уровень защиты не ниже 40.

Уровень 40 обеспечивает дополнительную защиту целостности без снижения производительности системы. Приложения, не выполняющиеся на уровне 40, снижают производительность системы на уровне защиты 30. В результате их работы система должна отвечать на нарушения домена.

Уровень защиты 50 предназначен для систем с очень высокими требованиями к защите. Система, работающая на уровне защиты 50, выполняет дополнительные проверки, иногда влияющие на производительность.

Даже если вы собираетесь предоставить всем пользователям права доступа ко всей информации, рекомендуется применять уровень защиты 30. Доступ ко всей информации можно предоставить с помощью общих прав доступа. Если с самого начала применять уровень защиты 30, то это позволит защитить особо важные ресурсы, когда это потребует, без повторного тестирования всех приложений.

Понятия, связанные с данным

“Уровень защиты” на стр. 2

Платформа System i поддерживает пять уровней защиты. С помощью системного значения Уровень защиты (QSECURITY) вы можете задать уровень защиты системы.

Задачи, связанные с данной

“Выключение уровня защиты 50” на стр. 22

После перехода на уровень защиты 50 может возникнуть необходимость временно вернуться на уровень защиты 30 или 40, например, для тестирования новых приложений на предмет ошибок целостности.

Кроме того, вы можете обнаружить неполадки целостности, не возникавшие на более низких уровнях.

Уровень защиты 10

На уровне 10 защита выключена. Поэтому работать на этом уровне не рекомендуется.

Начиная с V4R3 переход на уровень защиты 10 невозможен. Если в системе изначально установлен уровень защиты 10, то при установке V4R3 это значение сохранится. Но если вы измените его на любое другое значение, то вернуться на уровень 10 уже не удастся.

При входе в систему нового пользователя система автоматически создает пользовательский профайл с именем, указанным в меню входа в систему. Если тот же пользователь позже войдет в систему с другим ИД пользователя, то будет создан другой пользовательский профайл. В таблице Приложение В, “Пользовательские профайлы, поставляемые IBM”, на стр. 337 перечислены значения по умолчанию, применяемые при автоматическом создании пользовательского профайла.

Проверка прав доступа выполняется на всех уровнях защиты. Так как пользовательским профайлам, созданным на уровне защиты 10, предоставляются специальные права доступа *ALLOBJ, то они успешно проходят почти все проверки прав доступа и получают доступ ко всем ресурсам системы. Для того чтобы определить возможные последствия перехода на более высокий уровень защиты, удалите специальные права доступа *ALLOBJ из пользовательских профайлов и предоставьте вместо них права доступа к конкретным ресурсам. Однако учтите, что фактический уровень защиты при этом не изменится. Для любого пользователя, указавшего при входе в систему новый ИД пользователя, будет создан пользовательский профайл со специальными правами доступа *ALLOBJ. На уровне защиты 10 избежать этого нельзя.

Уровень защиты 20

Уровень 20 обеспечивает лучшую защиту, чем уровень 10. Однако по умолчанию на уровне защиты 20 всем создаваемым пользовательским профайлам предоставляются специальные права доступа *ALLOBJ, поэтому работа на этом уровне не рекомендуется.

На уровне защиты 20 предусмотрены следующие функции защиты:

- Для входа в систему необходимо указать ИД пользователя и пароль.

- Пользовательские профайлы могут создавать администраторы и пользователи со специальными правами доступа *SECADM.
- Применяется значение Ограничить возможности, указанное в пользовательском профайле.

Переход с уровня 10 на уровень 20

При переходе с уровня 10 на уровень 20 все пользовательские профайлы, которые были автоматически созданы на уровне 10, сохраняются. Пароли пользовательских профайлов, созданных на уровне 10, совпадают с именами пользовательских профайлов. Специальные права доступа пользовательских профайлов не изменяются.

Ниже перечислены действия, которые рекомендуется выполнить при переходе рабочей системы с уровня 10 на уровень 20:

- Просмотрите список всех пользовательских профайлов системы с помощью команды Показать пользователей с правами доступа (DSPAUTUSR).
- Создайте новые пользовательские профайлы со стандартными именами или скопируйте существующие пользовательские профайлы и присвойте им новые, стандартные имена.
- Сделайте пароли всех существующих пользовательских профайлов устаревшими, чтобы пользователи изменили пароли.
- Укажите системные значения, определяющие правила составления паролей, таким образом, чтобы пользователи не могли вводить слишком простые пароли.
- Проверьте значения по умолчанию, приведенные в разделах “Значения по умолчанию для пользовательских профайлов” на стр. 337 и Приложение В, “Пользовательские профайлы, поставляемые IBM”, на стр. 337. При необходимости внесите изменения в профайлы, автоматически созданные на уровне 10.

Переход на уровень 20 с более высокого уровня

При переходе на уровень 20 с более высокого уровня в пользовательские профайлы добавляются специальные права доступа. В результате каждый пользователь получает, по крайней мере, специальные права доступа по умолчанию соответствующего класса пользователя.

При переходе на уровень 20 с более высокого уровня во все пользовательские профайлы добавляются специальные права доступа *ALLOBJ. Эти права доступа позволяют просматривать, изменять и удалять любые объекты системы.

Различия специальных прав доступа уровня 20 и более высоких уровней приведены в таблице Табл. 2 на стр. 11.

Уровень защиты 30

Уровень 30 обеспечивает лучшую защиту, чем уровень 20.

Помимо функций защиты уровня 20, на уровне защиты 30 предусмотрены следующие функции:

- Права доступа к ресурсам системы предоставляются отдельно каждому пользователю.
- Специальные права доступа *ALLOBJ автоматически предоставляются только пользовательским профайлам, созданным с помощью класса защиты *SECOFR.

Переход на уровень 30 с более низкого уровня

При переходе на уровень защиты 30 с более низкого уровня пользовательские профайлы изменяются после очередной IPL для обновления специальных прав доступа.

Специальные права доступа, предоставленные пользователю на уровнях 10 и 20, но недоступные на уровне 30, удаляются. Специальные права доступа, не связанные с классом пользователя, не изменяются. Например,

специальные права доступа *ALLOBJ удаляются из всех пользовательских профайлов, не принадлежащих классу пользователя *SECOFR. Специальные права доступа по умолчанию, а также различия между уровнем 10 или 20 и более высокими уровнями защиты приведены в таблице Табл. 2 на стр. 11.

Если на более низком уровне в системе выполнялись приложения, то перед переходом на уровень 30 рекомендуется настроить и проверить защиту ресурсов. Рекомендуется выполнить следующие действия:

- Задайте для всех приложений соответствующие права доступа к объектам.
- Проведите тестирование приложений с помощью реальных или пробных пользовательских профайлов.
 - На время тестирования удалите из этих пользовательских профайлов специальные права доступа *ALLOBJ.
 - Предоставьте пользовательским профайлам соответствующие права доступа к приложениям.
 - Запустите приложение от имени пользовательского профайла.
 - Проверьте наличие возможных сбоев, связанных с правами доступа. Для этого просмотрите сообщения об ошибках или воспользуйтесь журналом контроля за действиями.
- После успешного выполнения приложений от имени тестовых профайлов предоставьте соответствующие права доступа к объектам приложений рабочим пользовательским профайлам, которым требуется доступ к приложению.
- Если в системном значении QLMTSECOFR (Ограничить права системного администратора) указано значение 1 (Да), то на уровне защиты 30 и выше пользователям со специальными правами доступа *ALLOBJ и *SERVICE права доступа к устройствам предоставляются отдельно. Для этого предоставьте пользователям права доступа *CHANGE к выбранным устройствам, или добавьте права доступа *CHANGE в пользовательский профайл QSECOFR, или укажите 0 в системном значении QLMTSECOFR.
- Измените уровень защиты системы и выполните загрузку начальной программы (IPL).

Для того чтобы перейти на уровень 30 без определения прав доступа к отдельным объектам, задайте для объектов приложения общие права доступа, достаточно широкие для выполнения приложения. Убедитесь в отсутствии сбоев, связанных с правами доступа. Для этого выполните тестирование приложения.

Ссылки, связанные с данной

“Определение режима доступа к информации” на стр. 138

Можно указать, какие операции разрешены с объектами, данными и полями.

Уровень защиты 40

Уровень защиты 40 позволяет избежать нарушения целостности и повреждения защиты в результате работы программ, которые в некоторых случаях могут обходить защиту. Уровень защиты 50 обеспечивает дополнительную защиту целостности и предназначен для систем с жесткими требованиями к защите.

В таблице Табл. 3 приведено сравнение функций защиты, поддерживаемых на уровнях 30, 40 и 50.

Таблица 3. Сравнение уровней защиты 30, 40 и 50

Описание сценария	Уровень 30	Уровень 40	Уровень 50
Программа пытается получить доступ к объектам с помощью неподдерживаемых интерфейсов.	В журнал заносится запись AF ¹ .	В журнал заносится запись AF ¹ . Операция не выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.
Программа пытается выполнить запрещенную команду.	В журнал заносится запись AF ¹ . Операция не выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.
У пользователя, запускающего задание, нет прав доступа *USE к пользовательскому профайлу, указанному в описании задания.	В журнал заносится запись AF ¹ .	В журнал заносится запись AF ¹ . Задание не запускается.	В журнал заносится запись AF ¹ . Задание не запускается.

Таблица 3. Сравнение уровней защиты 30, 40 и 50 (продолжение)

Описание сценария	Уровень 30	Уровень 40	Уровень 50
Пользователь пытается выполнить вход в систему по умолчанию, не вводя ИД пользователя и пароль.	В журнал заносится запись AF ¹ .	В журнал заносится запись AF ¹ . Вход в систему не выполняется.	В журнал заносится запись AF ¹ . Вход в систему не выполняется.
Программа режима *USER пытается записать данные в системную область диска, доступ к которой разрешен только для чтения или запрещен.	Попытка может оказаться успешной.	В журнал заносится запись AF ¹ . Операция не выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.
Предпринята попытка восстановить программу, для которой не указано контрольное значение. ²	Проверка не выполняется. Для применения программы ее необходимо преобразовать.	Проверка не выполняется. Для применения программы ее необходимо преобразовать.	Проверка не выполняется. Для применения программы ее необходимо преобразовать.
Предпринята попытка восстановить программу, для которой указано контрольное значение.	Выполняется проверка программы.	Выполняется проверка программы.	Выполняется проверка программы.
Попытка изменения связанного пространства программы.	Операция выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.
Попытка изменения адресного пространства задания.	Операция выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.
Программа режима пользователя пытается вызвать программу системного домена или передать ей управление.	Операция выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.	В журнал заносится запись AF ¹ . Операция не выполняется.
Предпринята попытка создать объект пользовательского домена типа *USRSPC, *USRIDX или *USRQ в библиотеке, которая не указана в системном значении QALWUSRDMN.	Операция не выполняется.	Операция не выполняется.	Операция не выполняется.
Программа режима пользователя отправляет сообщение об исключительной ситуации программе режима системы, которая в стеке вызовов не расположена непосредственно над ней.	Операция выполняется.	Операция выполняется.	Операция не выполняется.
Программе пользовательского домена, работающей в режиме системы, передается параметр.	Операция выполняется.	Выполняется проверка параметра.	Выполняется проверка параметра.
Команда, поставляемая IBM, была изменена (с помощью команды CHGCMD) для запуска другой программы. Затем эта команда изменена еще раз, чтобы она запускала, как и прежде, исходную программу, поставляемую IBM, которая является программой системного домена. Пользователь пытается выполнить эту команду.	Операция выполняется.	В журнал заносится запись AF. ^{1,3} Операция не выполняется. ³	В журнал заносится запись AF. ^{1,3} Операция не выполняется. ³

Таблица 3. Сравнение уровней защиты 30, 40 и 50 (продолжение)

Описание сценария	Уровень 30	Уровень 40	Уровень 50
1	Если функция контроля активна, то в журнал контроля (QAUDJRN) заносится запись типа Сбой прав доступа (AF). Дополнительная информация о функции контроля приведена в разделе Глава 9, “Контроль эффективности защиты системы System i”, на стр. 271.		
2	Для программ, созданных в версиях ниже V1R3, контрольное значение не предусмотрено.		
3	После изменения команды, поставляемой IBM, она больше не может вызывать программу системного домена.		

В случае применения функции контроля на низких уровнях защиты система заносит в журнал записи о большинстве действий, перечисленных в таблице Табл. 3 на стр. 14, за исключением действий, обнаруженных функцией расширенной аппаратной защиты. Возможные нарушения целостности обозначаются предупреждениями в виде записей журнала. На уровне 40 и выше система не выполняет операции, которые могут привести к нарушению целостности.

Предотвращение использования неподдерживаемых интерфейсов

На уровне защиты 40 и выше система запрещает прямой вызов программ системы, не зарегистрированных в качестве интерфейсов вызовов.

Например, вы не сможете напрямую вызвать программу обработки команды SIGNOFF.

Для обеспечения этой защиты применяются атрибут домена, относящийся к объекту, и атрибут режима, относящийся к программе.

- **Домен:**

Все объекты, принадлежащие домену *SYSTEM или домену *USER. Объекты домена *SYSTEM доступны только для программ режима *SYSTEM, а также для программ режима *INHERIT, которые вызываются программами режима *SYSTEM.

Для просмотра домена объекта воспользуйтесь командой Показать описание объекта (DSPOBJD), указав в ней опцию DETAIL(*FULL). Кроме того, вы можете воспользоваться следующими командами:

- Показать программу (DSPPGM) - для просмотра домена программы
- Показать служебную программу (DPSRVPGM) - для просмотра домена служебной программы

- **Режим:**

Программы могут работать в одном из следующих режимов: *SYSTEM, *INHERIT или *USER. Программы режима *USER напрямую могут обращаться только к объектам домена *USER. Объекты домена *SYSTEM становятся доступными только с помощью соответствующей команды или интерфейса прикладных программ (API). Режимы *SYSTEM и *INHERIT зарезервированы для программ, поставляемых IBM.

Для просмотра режима программы воспользуйтесь командой Показать программу (DSPPGM). Для просмотра режима служебной программы воспользуйтесь командой Показать служебную программу (DPSRVPGM).

В таблице Табл. 4 перечислены правила предоставления прав доступа в зависимости от домена и режима:

Таблица 4. Права доступа в зависимости от домена и режима

Состояние программы	Домен объекта	
	*USER	*SYSTEM
*USER	ДА	Нет ¹
*SYSTEM	ДА	ДА

Таблица 4. Права доступа в зависимости от домена и режима (продолжение)

Состояние программы	Домен объекта	
	*USER	*SYSTEM
¹ Нарушение домена или режима вызывает сбой операции на уровне защиты 40 и выше. Если функция контроля активна, то записи типа AF заносятся в журнал контроля на всех уровнях защиты.		

Запись журнала:

Если выполнены следующие условия, то в журнал QAUDJRN заносится запись Сбой прав доступа (AF), в которой указано нарушение типа D или R.

- Функция контроля включена
- Системное значение QAUDLVL содержит *PGMFAIL
- Выполняется обращение к неподдерживаемому интерфейсу

Защита описаний заданий

Если в поле Пользователь описания задания указано имя пользовательского профайла, то все задания, переданные на выполнение с этим описанием задания, могут применять этот пользовательский профайл. С помощью описания задания несанкционированный пользователь может передать задание на выполнение от имени пользовательского профайла, указанного в этом описании.

На уровне защиты 40 и выше для передачи задания на выполнение пользователю необходимы права доступа *USE как к описанию задания, так и к пользовательскому профайлу, указанному в этом описании. В противном случае, задание выполнено не будет. На уровне защиты 30 задание будет выполнено, если у пользователя, передающего его на выполнение, есть права доступа *USE к описанию этого задания.

Запись журнала:

Если выполнены следующие условия, то в журнал QAUDJRN заносится запись AF, в которой указано нарушение типа J.

- Функция контроля включена
- Системное значение QAUDLVL содержит *AUTFAIL
- У пользователя, передающего задание на выполнение, нет прав доступа к пользовательскому профайлу, указанному в описании задания.

Вход в систему без ИД пользователя и пароля

Способ входа в систему без ИД пользователя и пароля определяется на основе уровня защиты.

На уровне защиты 30 и ниже некоторые описания подсистемы позволяют войти в систему без указания ИД пользователя. На уровне 40 и выше вход в систему без указания ИД пользователя и пароля невозможен.

Запись журнала:

Если выполнены следующие условия, то в журнал QAUDJRN заносится запись AF, в которой указано нарушение типа S.

- Функция контроля включена
- Системное значение QAUDLVL содержит *AUTFAIL
- Пользователь пытается войти в систему без указания ИД пользователя и пароля, и это действие разрешено описанием подсистемы.

На уровне защиты 40 и выше данное действие запрещено.

Понятия, связанные с данным

“Описания подсистем” на стр. 215

Описания подсистем применяются для различных функций в системе.

Расширенная аппаратная защита памяти

Расширенная аппаратная защита памяти позволяет определить блоки системной информации, расположенные в памяти, как доступные для чтения и записи, доступные только для чтения или недоступные.

На уровне 40 и выше доступом программ режима *USER к защищенным блокам управляет система.

Расширенная аппаратная защита памяти поддерживается на всех моделях System i.

Запись журнала:

Если выполнены следующие условия, то в журнал QAUDJRN заносится запись AF, в которой указано нарушение типа R.

- Функция контроля включена
- Системное значение QAUDLVL содержит *PGMFAIL
- Программа пытается записать данные в область жесткого диска, защищенную с помощью расширенной аппаратной защиты памяти.

Защита области программы

Для программ исходной модели программ (OPM) на уровне защиты 40 и выше программа режима пользователя не может напрямую изменить область, связанную с программным объектом. Для программ интегрированной языковой среды (ILE) на любом уровне защиты программа режима пользователя не может изменить область, связанную с программным объектом.

Защита адресного пространства задания

На уровне защиты 50 программа режима пользователя не может получить адрес другого задания системы. По этой причине, программа в режиме пользователя не может напрямую работать с объектами, связанными с другими заданиями.

Проверка параметров

В пользовательском домене роль интерфейсов операционной системы i5/OS играют программы режима системы. Параметры, передаваемые программой режима пользователя программе режима системы, необходимо проверять, так как непредвиденные значения могут нарушить целостность операционной системы.

На уровне 40 или 50 отдельно проверяется каждый параметр, передаваемый программами режима пользователя программам режима системы в пользовательском домене. В соответствии с требованиями уровня защиты Common Criteria пользовательский и системный домены должны быть разделены. Так как в ходе проверки выполняются дополнительные операции, производительность системы может снизиться.

Проверка восстанавливаемых программ

При создании программы система вычисляет контрольное значение, которое сохраняется вместе с программой. В процессе восстановления программы контрольное значение вычисляется вновь и сравнивается с контрольным значением, сохраненным с программой.

Если значения при проверке не совпадают, то система выполняет действия согласно системным значениям Преобразование при восстановлении (QFRCCVNRST) и Разрешить восстановление объекта (QALWOBJRST).

Помимо контрольного значения, программу можно защитить с помощью цифровой подписи, проверяемой при восстановлении. Все действия системы, связанные с цифровыми подписями, контролируются системными значениями QVFYOBJRST и QFRCCVNRST. Системные значения Проверять

восстанавливаемые объекты (QVFYOBJRST), QFRCCVNRST и QALWOBJRST играют роль фильтров, определяющих, следует ли восстановить программу без изменений, повторно создать (преобразовать) ее при восстановлении или запретить восстановление.

Примечание: Программы режима системы должны иметь правильную цифровую подпись IBM. В противном случае их восстановление будет невозможно при любых системных значениях

Первый фильтр - это системное значение QVFYOBJRST. Оно управляет операцией восстановления подписанных объектов. После успешной проверки объекта с помощью этого системного значения объект передается второму фильтру - системному значению QFRCCVNRST. Это системное значение позволяет указать необходимость преобразования программ, служебных программ и объектов модулей в процессе восстановления. Кроме того, это системное значение запрещает восстановление некоторых объектов. Объекты передаются третьему - последнему - фильтру, системному значению QALWOBJRST, только в том случае, если они успешно прошли первые два фильтра. Это системное значение определяет, следует ли восстанавливать объекты с конфиденциальными атрибутами.

Notes:

1. Программы, разработанные для операционной системы i5/OS, могут содержать информацию, на основе которой система может заново создать программу в процессе ее восстановления, не имея ее исходного текста.
2. Программы, разработанные для i5/OS версии V5R1 и выше, содержат информацию, которая позволяет заново создать программу даже в том случае, если информация наблюдаемости программы была удалена.
3. Программы, разработанные для более ранних выпусков, могут быть заново созданы в процессе восстановления только в том случае, если наблюдаемость сохранилась.

Ссылки, связанные с данной

“Системные значения, связанные с защитой” на стр. 39

В этом разделе описаны системные значения, связанные с защитой операционной системы i5/OS.

Переход на уровень защиты 40

Перед переходом на уровень 40 убедитесь в правильной работе всех необходимых приложений на уровне 30. Уровень защиты 30 позволяет протестировать защиту ресурсов во всех приложениях.

Для перехода на уровень защиты 40 выполните следующие действия:

1. Активируйте функцию контроля за действиями, если вы еще не сделали этого. Полный набор инструкций по настройке функции контроля приведен в разделе “Настройка контроля за действиями” на стр. 308.
2. Убедитесь, что в системном значении QAUDLVL указаны значения *AUTFAIL и *PGMFAIL. Значение *PGMFAIL позволяет заносить в журнал записи обо всех попытках доступа, нарушающих целостность защиты на уровне 40.
3. Отслеживайте все записи *AUTFAIL и *PGMFAIL, заносимые в журнал контроля, при выполнении всех приложений на уровне защиты 30. Особое внимание обратите на следующие коды причин в записях AF:

C	Сбой, связанный с проверкой объекта
D	Нарушение, связанное с неподдерживаемым интерфейсом (доменом)
J	Сбой, связанный с правами доступа описания задания и пользовательского профайла
Ч	Попытка обращения к защищенной области жесткого диска (расширенная аппаратная защита памяти)
S	Попытка входа в систему по умолчанию

Данные коды указывают на существование возможных нарушений целостности в приложениях. На уровне защиты 40 выполнение таких программ запрещено.

4. Команда CHGPGM с параметром FRCCRT позволяет создать контрольные значения для программ, созданных в версиях до V1R3. На уровне защиты 40 система транслирует все программы, восстанавливаемые без контрольных значений. Это может значительно замедлить процесс восстановления. Дополнительная информация о проверке программ приведена в разделе “Проверка восстанавливаемых программ” на стр. 18.

Примечание: В процессе тестирования приложения восстановите библиотеки программы. Проверьте наличие записей об ошибках проверки в журнале контроля.

5. В соответствии с записями, занесенными в журнал контроля, выполните действия по исправлению приложений и предотвращению сбоев программ.
6. Укажите 40 в системном значении QSECURITY и выполните IPL.

Выключение уровня защиты 40

Иногда необходимо вернуться на уровень защиты 30 с уровня 40, например, для проверки целостности новых приложений. Кроме того, может оказаться, что перед переходом на уровень 40 тестирование было выполнено не полностью.

Переход с уровня 40 на уровень 30 можно выполнить, не подвергая опасности защиту ресурсов. При переходе с уровня 40 на уровень 30 специальные права доступа пользовательских профайлов не изменяются. После тестирования приложений или исправления ошибок, занесенных в журнал контроля, вы можете вернуться на уровень 40.

Внимание: В случае перехода с уровня 40 на уровень 20 во все пользовательские профайлы добавляются специальные права доступа. (См. Табл. 2 на стр. 11.) При этом ресурсы становятся незащищенными.

Уровень защиты 50

Уровень защиты 50 разработан в соответствии с некоторыми требованиями, предъявляемыми Controlled Access Protection Profile (CAPP) для защиты Common Criteria (CC). Уровень защиты 50 обеспечивает дополнительную защиту целостности в дополнение к защите уровня 40 и предназначен для систем с жесткими требованиями к защите.

Описание функций защиты на уровне 50 приведено в следующих разделах:

- Ограничения на типы объектов пользовательского домена (*USRSPC, *USRIDX и *USRQ)
- Ограничения на обработку сообщений, передаваемых между программами режима системы и режима пользователя
- Запрет на изменение всех внутренних управляющих блоков

Ограничения на объекты пользовательского домена

Большинство объектов создаются в системном домене. На уровнях защиты 40 и 50 работать с объектами системного домена можно только с помощью предоставленных команд и API.

Следующие объекты могут принадлежать как системному, так и пользовательскому домену:

- Пользовательское пространство (*USRSPC)
- Пользовательский индекс (*USRIDX)
- Пользовательская очередь (*USRQ)

С объектами *USRSPC, *USRIDX и *USRQ пользовательского домена можно работать напрямую без применения поставляемых API и команд. Такой подход позволяет обратиться к объекту без создания контрольной записи.

Примечание: В пользовательском домене также поддерживаются объекты типа *PGM, *SRVPGM и *SQLPKG. Содержимое этих объектов нельзя изменить напрямую и к ним неприменимы ограничения.

На уровне защиты 50 у пользователя не должно быть возможности передавать конфиденциальную информацию другим пользователям без отправки контрольной записи. Для этого должны выполняться следующие условия:

- На уровне защиты 50 задания не могут получать доступ к библиотеке QTEMP другого задания. Поэтому, если объекты пользовательского домена хранятся в библиотеке QTEMP, с их помощью нельзя передавать информацию другим пользователям.
- Для обеспечения совместимости с существующими приложениями, применяющими объекты пользовательского домена, вы можете указать дополнительные библиотеки в системном значении QALWUSRDMN. Системное значение QALWUSRDMN применяется на всех уровнях защиты. Дополнительная информация приведена в разделе “Разрешить объекты пользовательского домена (QALWUSRDMN)” на стр. 27.

Задачи, связанные с данной

“Переход на уровень защиты 50” на стр. 22

Если текущий уровень защиты - это 10 или 20, перейдите сначала на уровень 40 и затем на уровень 50.

Если текущий уровень защиты - это 30 или 40, то требуется вычислить значение QALWUSRDMN и перекомпилировать некоторые программы, чтобы подготовить их для уровня 50.

Ограничения на обработку сообщений

Сообщения, пересылаемые между программами, могут представлять угрозу для целостности системы.

На уровне защиты 50 можно ограничить пересылку сообщений между программами для защиты целостности системы.

Обработка сообщений на уровне 50 выполняется в соответствии со следующими правилами:

- Любая программа режима пользователя может отправлять сообщения любой другой программе режима пользователя.
- Любая программа режима системы может отправлять сообщения любой другой программе режима пользователя или системы.
- Любая программа режима системы может отправлять сообщения любой другой программе режима системы, кроме сообщений об исключительных ситуациях.
- Программа режима пользователя может отправлять сообщения об исключительных ситуациях (сообщения о состоянии, уведомления или аварийные сообщения) программе режима системы, если выполняется одно из следующих условий:
 - Программа режима системы является обработчиком запросов.
 - Программа режима системы вызвала программу режима пользователя.

Примечание: Для отправки сообщения об исключительной ситуации программа режима пользователя не обязательно должна быть вызвана программой режима системы. Например, в данном стеке вызовов программы В, С и D могут отправить сообщение об исключительной ситуации программе А:

Программа А	Режим системы
Программа В	Режим пользователя
Программа С	Режим пользователя
Программа D	Режим пользователя

- Когда программа режима пользователя получает сообщение из внешнего источника (*EXT), из текста замещения сообщения удаляются все указатели.

Запрет на изменение внутренних управляющих блоков

На уровне защиты 40 некоторые внутренние управляющие блоки, например управляющий блок работы, нельзя изменить с помощью программы режима пользователя. На уровне защиты 50 запрещено изменение всех внутренних управляющих блоков, включая путь к открытым данным (ODP), области команд CL и программ и управляющий блок заданий среды S/36.

Переход на уровень защиты 50

Если текущий уровень защиты - это 10 или 20, перейдите сначала на уровень 40 и затем на уровень 50. Если текущий уровень защиты - это 30 или 40, то требуется вычислить значение QALWUSRDMN и перекомпилировать некоторые программы, чтобы подготовить их для уровня 50.

Как правило, дополнительные средства защиты, применяемые на уровне 50, не вносят записи в журнал контроля на более низких уровнях защиты. По этой причине, полное тестирование приложения на предмет всевозможных ошибок целостности возможно только после перехода на уровень 50.

Действия, приводящие к ошибкам на уровне 50, не свойственны обычным приложениям. Как правило, приложение, успешно работающее на уровне 40, будет работать и на уровне 50.

Для того чтобы подготовить систему к переходу с уровня 30 на уровень 50, выполните действия, приведенные в разделе “Переход на уровень защиты 40” на стр. 19.

Для того чтобы подготовить систему к переходу с уровня 30 или 40 на уровень 50, выполните следующие действия:

- Определите системное значение QALWUSRDMN. Управление объектами пользовательского домена играет важную роль в обеспечении целостности системы.
- Перекомпилируйте все программы на языке COBOL, присваивающие устройству значение WORKSTATION в предложении SELECT, если ранее они были обработаны компилятором версии ниже V2R3.
- Перекомпилируйте все программы на языке COBOL среды S/36, ранее обработанные компилятором версии ниже V2R3.
- Перекомпилируйте все программы на языке RPG/400 и программы на языке RPG* среды System/38, применяющие файлы дисплеев, если ранее они были обработаны компилятором версии ниже V2R2.

На уровень 50 можно перейти непосредственно с уровня 30. Промежуточное тестирование на уровне 40 выполнять не обязательно.

Для перехода с уровня 40 на уровень 50 дополнительное тестирование не требуется. Уровень 50 невозможно протестировать заранее. Дополнительная защита целостности, применяемая на уровне 50, не приводит к выдаче сообщений об ошибках и занесению записей в журнал на более низких уровнях защиты.

Понятия, связанные с данным

“Ограничения на объекты пользовательского домена” на стр. 20

Большинство объектов создаются в системном домене. На уровнях защиты 40 и 50 работать с объектами системного домена можно только с помощью предоставленных команд и API.

Выключение уровня защиты 50

После перехода на уровень защиты 50 может возникнуть необходимость временно вернуться на уровень защиты 30 или 40, например, для тестирования новых приложений на предмет ошибок целостности. Кроме того, вы можете обнаружить неполадки целостности, не возникавшие на более низких уровнях.

Переход с уровня 50 на уровень 30 или 40 можно выполнить, не подвергая опасности защиту ресурсов. При переходе с уровня 50 на уровень 30 или 40 специальные права доступа пользовательских профайлов не изменяются. После тестирования приложений или исправления ошибок, занесенных в журнал контроля, вы можете вернуться на уровень 50.

Внимание: В случае перехода с уровня 50 на уровень 20 во все пользовательские профайлы добавляются специальные права доступа. При этом ресурсы становятся незащищенными.

Ссылки, связанные с данной

Глава 2, “Работа с системным значением Защита системы (QSecurity)”, на стр. 9

С помощью системного значения Уровень защиты (QSECURITY) вы можете задать степень защищенности системы.

Глава 3. Системные значения защиты

Системные значения позволяют настроить различные характеристики системы. Для определения общесистемных параметров защиты предусмотрена группа системных значений.

При необходимости вы можете ограничить доступ к системным значениям, связанным с защитой. Соответствующие опции предусмотрены в Системном инструментарии (SST) и Специальных сервисных средствах (DST). Блокировка системных значений позволяет запретить их изменение с помощью команды CHGSYSVAL даже пользователям, обладающим правами доступа *SECADM и *ALLOBJ. Кроме запрета изменения этих системных значений, с помощью API Добавить проверку вы можете ограничить права доступа на добавление цифровых сертификатов в хранилище сертификатов, а также на сброс пароля хранилища цифровых сертификатов.

Примечание: Обратите внимание, что для выполнения операции по восстановлению в ходе восстановления системы блокировку системных значений необходимо отменить. Это позволит внести изменения в системные значения при выполнении IPL.

Опция блокировки позволяет ограничить следующие системные значения:

Таблица 5. Системные значения, которые можно блокировать

QALWJOBITP	QAUTORMT	QLMTDEVSSN	QPWDLMTREP	QRETSVRSEC
QALWOBJRST	QAUTOVRT	QLMTSECOFR	QPWDLVL	QRMTSIGN
QALWUSRDMN	QCRTAUT	QMAXSGNACN	QPWDMAXLEN	QRMTSRVATR
QAUDCTL	QCRTOJAUD	QMAXSIGN	QPWDMINLEN	QSCANFS
QAUDENACN	QDEVRCYACN	QPWDCHGBLK	QPWDPOSDIF	QSCANFSCTL
QAUDFRCLVL	QDSPSGNINF	QPWDEXPITV	QPWDRQDDGT	QSECURITY
QAUDLVL	QDSCJOBITV	QPWDEXPWRN	QPWDRQDDIF	QSHRMEMCTL
QAUDLVL2	QFRCCVNRST	QPWDLMTAJC	QPWDRULES	QUSEADPAUT
QAUTOCFG	QINACTMSGQ	QPWDLMTCHR	QPWDVLDPGM	QVFYOBJRST

Блокировать и отменить блокировку системных значений, связанных с защитой, можно с помощью Системного инструментария (SST) или Специальных сервисных средств (DST). Однако в режиме восстановления доступны только Специальные сервисные средства (DST). В противном случае, рекомендуется работать с SST.

Для того чтобы блокировать или разблокировать системные значения, связанные с защитой, с помощью команды Запустить системный инструментарий (STRSST) выполните следующие действия:

Примечание: Для этого вам потребуются ИД пользователя и пароль сервисных средств.

1. Откройте командную строку.
2. В командной строке введите STRSST.
3. Введите ИД пользователя и пароль сервисных средств.
4. Выберите опцию 7 (Работа с защитой системы).
5. В параметре **Разрешить изменения системных значений защиты** укажите 1 для разблокировки системных значений, связанных с защитой, или 2 для их блокировки.

Для того чтобы заблокировать или разблокировать системные значения, связанные с защитой, с помощью Специальных сервисных средств (DST) во ходе контролируемой IPL восстановления системы выполните следующие действия:

1. Выберите опцию 3 (Работа со Специальными сервисными средствами) в меню IPL или Установить систему.

Примечание: Данный этап предполагает, что система находится в режиме восстановления и выполняется контролируемая IPL.

2. Введите ИД пользователя и пароль сервисных средств.
3. Выберите опцию 13 (Работа с защитой системы).
4. В параметре **Разрешить изменения системных значений защиты** укажите 1 для разблокировки системных значений, связанных с защитой, или 2 для их блокировки.

Понятия, связанные с данным

“Системные значения” на стр. 3

Системные значения позволяют настроить многие параметры платформы System i. Системные значения можно использовать для указания глобальных параметров защиты.

Общие системные значения защиты

В этом разделе описаны общие системные значения, которые можно использовать для управления защитой в операционной системе i5/OS.

Описание:

Общие системные значения защиты позволяют настроить функции защиты, обеспечивающие выполнение принятой стратегии защиты. Например, в стратегии могут быть указано, что системы, содержащие конфиденциальную информацию, такую как счета клиентов или реестр фондов, требуют более надежной защиты, чем системы, применяемые для тестирования приложений в компании. Защиту этих систем можно настроить в соответствии с требованиями, указанными в стратегии защиты.

Задача:

Системные значения, управляющие защитой системы.

Средства для ее решения:

WRKSYSVAL *SEC (команда Работа с системными значениями)

Права доступа:

*ALLOBJ и *SECADM

Запись в журнале:

SV

Прим.: Изменения вступают в силу немедленно. IPL требуется только для изменения уровня защиты (системное значение QSECURITY) или уровня пароля (системное значение QPWDVLV).

Ниже приведены общие системные значения, управляющие защитой системы:

QALWUSRDMN

Разрешить объекты пользовательского домена в библиотеках

QCRTAUT

Создать общие права доступа по умолчанию

QDSPSGNINF

Показать информацию о входе в систему

QFRCCVNRST

Преобразование при восстановлении

QINACTITV

Тайм-аут для неактивного задания

QINACTMSGQ

Очередь сообщений неактивного задания

QLMTDEVSSN

Ограничить сеансы одним устройством

QLMTSECOFR

Ограничить права системного администратора

QMAXSIGN

Максимальное число попыток входа в систему

QMAXSGNACN

Действие при достижении максимального числа попыток входа в систему

QRETSVRSEC

Сохранять идентификационные данные на сервере

QRMTSIGN

Управление удаленным входом в систему

QSCANFS

Сканирование файловых систем

QSCANFSCTL

Управление сканированием файловых систем

QSECURITY

Уровень защиты

QSHRMEMCTL

Управление общей памятью

QUSEADPAUT

Применять принятые права доступа

QVIFYOVRST

Проверять восстанавливаемые объекты

Разрешить объекты пользовательского домена (QALWUSRDMN)

При создании всем объектам присваивается атрибут домена. Домен - это характеристика объекта, управляющая доступом программ к объекту. Системное значение Разрешить объекты пользовательского домена (QALWUSRDMN) позволяет указать библиотеки, которые могут содержать объекты пользовательского домена типа *USRSPC, *USRIDX или *USRQ.

Ограничение объектов *USRSPC, *USRIDX и *USRQ является обязательным для систем с высокими требованиями к защите. Система не может контролировать входящие и исходящие потоки информации объектов пользовательского домена. Ограничение не применяется к объектам пользовательского домена типа программа (*PGM), программа сервера (*SRVPGM) или пакеты SQL (*SQLPKG).

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 6. Для системного значения QALWUSRDMN предусмотрены следующие значения:

*ALL	Объекты пользовательского домена разрешены во всех библиотеках и каталогах системы. Это поставляемое значение.
*DIR	Объекты пользовательского домена разрешены во всех каталогах системы.
<i>имя-библиотеки</i>	Имена до 50 библиотек, которые могут содержать объекты пользовательского домена типа *USRSPC, *USRIDX или *USRQ. В список отдельных библиотек <i>должна</i> выходить библиотека QTEMP.

Рекомендуемое значение: В большинстве случаев рекомендуется указывать значение *ALL. Для систем с высокими требованиями к защите объекты пользовательского домена должны быть разрешены только в библиотеке QTEMP.

В некоторых системах установлено прикладное программное обеспечение, работа которого основана на объектах *USRSPC, *USRIDX и *USRQ. В таких случаях в список библиотек системного значения QALWUSRDMN должны входить библиотеки, применяемые этим прикладным программным обеспечением. Для всех библиотек системного значения QALWUSRDMN, кроме QTEMP, для общих прав доступа должно быть указано значение *EXCLUDE. Это позволяет ограничить число неконтролируемых пользователей, применяющих интерфейс MI для чтения данных и изменения данных объектов пользовательского домена в этих библиотеках.

Примечание: Выполнение команды Восстановить память (RCLSTG) может потребовать перемещения объектов пользовательского домена из библиотеки QRCL (восстановить память) или в нее. Для успешного выполнения команды RCLSTG может потребоваться добавить библиотеку QRCL в системное значение QALWUSRDMN. По соображениям защиты рекомендуется для общих прав доступа к библиотеке QRCL указать значение *EXCLUDE. После выполнения команды RCLSTG удалите библиотеку QRCL из системного значения QALWUSRDMN.

Права доступа к новым объектам (QCRTAUT)

Системное значение Права доступа к новым объектам (QCRTAUT) указывает общие права доступа к вновь создаваемым объектам.

Системное значение QCRTAUT позволяет определить общие права доступа для новых объектов, если выполняются следующие условия:

- В системном значении Права при создании (CRTAUT) для библиотеки нового объекта указано значение *SYSVAL.
- Новый объект создается с общими правами доступа (AUT) *LIBCRTAUT.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 7. Для системного значения QCRTAUT предусмотрены следующие значения:

*CHANGE	Обычные пользователи могут изменять новые объекты.
*USE	Обычные пользователи могут просматривать, но не изменять общие объекты.
*ALL	Обычные пользователи могут выполнять над новыми объектами любые действия.
*EXCLUDE	Обычным пользователям запрещено работать с новыми объектами.

Рекомендуемое значение:
*CHANGE

Системное значение QCRTAUT не применяется для объектов, созданных в каталогах расширенной файловой системы.

Внимание: Для некоторых библиотек, поставляемых IBM, включая QSYS, в CRTAUT указано значение *SYSVAL. Если изменить системное значение QCRTAUT на значение, отличное от *CHANGE, могут возникнуть неполадки, связанные с входом в систему с помощью новых или автоматически созданных устройств. Для того чтобы избежать этих неполадок при изменении QCRTAUT на значение, отличное от *CHANGE, следует убедиться, что для общих прав доступа описаний всех устройств и связанных с ними очередей сообщений указано значение *CHANGE. Для этого можно, к примеру, изменить значение CRTAUT для библиотеки QSYS с *SYSVAL на *CHANGE.

Показать информацию о входе в систему (QDSPSGNINF)

Системное значение Показать информацию о входе в систему (QDSPSGNINF) определяет, следует ли после входа в систему отображать информацию о входе в систему.

Отображается следующая информация о входе в систему:

- Дата последнего входа в систему
- Ошибки проверки пароля
- Число дней до истечения срока действия пароля (если до этого момента осталось меньше допустимого числа дней)

Информация о входе в систему

Система:

Предыдущий вход в систему : 10/30/91 14:15:00

Число ошибок проверки пароля : 3

Число дней до истечения срока действия пароля: 5

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 8. Для системного значения QDSPSGNINF предусмотрены следующие значения:

<u>0</u>	Информация не отображается.
<u>1</u>	Информация отображается.

Рекомендуемое значение: 1 (Информация отображается). Это значение позволяет пользователям отслеживать применение своих пользовательских профайлов, а также иметь представление о сроке действия пароля.

Примечание: Указать необходимость отображения информации о входе в систему можно также в отдельных пользовательских профайлах.

Тайм-аут для неактивного задания (QINACTITV)

Системное значение Тайм-аут для неактивного задания (QINACTITV) задает время в минутах, в течение которого система не выполняет действия по обработке неактивного задания.

Рабочая станция считается неактивной, если она находится в состоянии ожидания дисплея (DSPW) или ожидает ввода сообщения или действий пользователя в меню. Некоторые примеры действий пользователей:

- Нажатие клавиши Enter
- Применение функции подкачки
- Нажатие функциональных клавиш

- Нажатие клавиши Справка

Сеансы эмуляции с помощью System i Access также учитываются. Локальные задания, выполняемые в удаленной системе, не учитываются. Задания, подключенные по протоколу передачи файлов (FTP), не учитываются. Для управления тайм-аутом соединений FTP измените параметр INACTTIMO в команде Изменить атрибут FTP (CHGFTP). Для управления тайм-аутом соединений Telnet до V4R2 воспользуйтесь командой Изменить атрибут Telnet (CHGTELNA).

Ниже приведены примеры того, каким образом система определяет неактивные задания:

- Функция Системный запрос позволяет запустить второе интерактивное задание. В результате действия пользователя, такого как нажатие клавиши Enter, в одном из заданий оба задания помечаются как активные.
- Задание System i Access может стать неактивным, если пользователь выполняет на своем компьютере такие действия, как редактирование документа, без взаимодействия с системой.

Системное значение QINACTMSGQ определяет действие, выполняемое над неактивным заданием, после истечения указанного времени.

После запуска система проверяет наличие неактивных заданий с частотой, указанной в системном значении QINACTITV. Например, если система запущена в 9:46 утра и в системном значении QINACTITV указано 30 минут, то она проверяет наличие неактивных заданий в 10:16, 10:46, 11:16 и т.д. Если задание неактивно в течение 30 минут, то выполняется действие, указанное в системном значении QINACTMSGQ. В этом примере задание, ставшее неактивным в 10:17, будет обработано только в 11:16. В ходе проверки, выполненной в 10:46, было определено, что это задание было неактивным только в течение 29 минут.

Системные значения QINACTITV и QINACTMSGQ обеспечивают защиту подключенных рабочих станций, так как они не позволяют пользователями покидать их. Неактивная рабочая станция может служить причиной несанкционированного доступа к системе.

Таблица 9. Для системного значения QINACTITV предусмотрены следующие значения:

*NONE:	Система не проверяет наличие неактивных заданий.
<i>время-в-минутах</i>	Укажите значение от 5 до 300. Если задание неактивно в течение этого времени, выполняется действие, указанное в QINACTMSGQ.

Рекомендуемое значение: 60 минут

Очередь сообщений неактивного задания (QINACTMSGQ)

Системное значение Очередь сообщений неактивного задания (QINACTMSGQ) определяет действие, выполняемое над неактивным заданием после истечения указанного времени.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 10. Для системного значения QDEVRCYACN предусмотрены следующие значения:

*ENDJOB	Неактивные задания завершаются. Если неактивное задание представляет собой групповое задание, ¹ то закрываются все задания, связанные с этой группой. Если задание входит в состав вспомогательного задания, ¹ то завершаются оба задания. Действие *ENDJOB над неактивным заданием аналогично запуску команды ENDJOB JOB(имя) OPTION (*IMMED) ADLINTJOBS(*ALL).
----------------	--

Таблица 10. Для системного значения QDEVRCYACN предусмотрены следующие значения: (продолжение)

*DSCJOB	<p>Неактивное задание отключается. Вместе с ним отключаются все вспомогательные и групповые задания, ¹ связанные с ним. Системное значение Тайм-аут для отключенного задания (QDSCJOBTV) позволяет завершить отключенные задания. Дополнительная информация приведена в разделе “Тайм-аут для отключенного задания (QDSCJOBTV)” на стр. 42.</p> <p>Внимание: Некоторые задания, такие как PC Organizer или Текстовая поддержка PC (PCTA), отключить невозможно. Если система не может отключить неактивное задание, оно завершается.</p>
имя-очереди-сообщений	<p>При достижении тайм-аута в указанную очередь сообщений отправляется сообщение CPI1126. В этом сообщении указывается следующая информация: Задание &3/&2/&1; неактивно.</p> <p>Очередь, указанная в системном значении QINACTMSGQ, должна существовать. В ходе IPL эта очередь сообщений автоматически очищается. Если указать в системном значении QINACTMSGQ пользовательскую очередь сообщений, то при каждой IPL все сообщения из нее будут удаляться.</p>
<p>¹ В разделе Управление заданиями описаны групповые задания и вторичные задания.</p>	

Рекомендуемое значение: *DSCJOB, если пользователи не работают с заданиями System i Access. Если значение *DSCJOB применяется для заданий System i Access, то эти задания завершаются. Это может привести к значительной потере информации. Для лицензионных программ System i Access рекомендуется применять опцию *очередь-сообщений*. В разделе Программирование на CL приведен пример создания программы, обрабатывающей сообщения.

Работа с очередью сообщений: Очередь сообщений можно отслеживать вручную или автоматически. В случае обнаружения неактивного задания выполняется необходимое действие, такое как завершение задание или отправка предупреждающего сообщения пользователю. Очередь сообщений позволяет обрабатывать неактивные устройства различными способами, в зависимости от типа устройства или пользовательского профайла. Такой подход рекомендуется в случае применения лицензионных программ System i Access.

Если в рабочей станции неактивны два задания, то в очередь сообщений отправляются два сообщения (одно для каждого вспомогательного задания). Завершить одно или оба вспомогательных задания можно вручную, либо автоматически с помощью команды Завершить задание (ENDJOB). Если неактивное задание связано с групповыми заданиями, то в очередь сообщений отправляется одно сообщение. Сообщения отправляются в очередь сообщений с частотой, указанной для тайм-аута.

Ограничить сеансы одним устройством (QLMTDEVSSN)

Системное значение Ограничить сеансы одним устройством (QLMTDEVSSN) указывает, ограничено ли число сеансов с устройствами для пользователя.

Это значение не ограничивает меню Системный запрос одного устройства и не запрещает второй вход в систему с его помощью. Пользователь может войти в систему с помощью другого устройства после отключения предыдущего задания.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 11. Для системного значения QLMTDEVSSN предусмотрены следующие значения:

0	Для пользователя нет ограничений на число сеансов с устройствами.
1	Пользователю разрешен один сеанс с устройством.

Таблица 11. Для системного значения QLMTDEVSSN предусмотрены следующие значения: (продолжение)

2 - 9	Пользователю разрешено указанное число сеансов с устройствами.
-------	--

Рекомендуемое значение: 1 (Да). Ограничение сеансов одним устройством снижает вероятность использования одинаковых паролей и того, что устройства останутся без присмотра.

Примечание: Необходимость ограничения сеансов одним устройством можно также указать в отдельных пользовательских профайлах.

Ограничить права доступа системного администратора (QLMTSECOFR)

Системное значение Ограничить права доступа системного администратора (QLMTSECOFR) позволяет указать, разрешено ли пользователям с правами доступа ко всем объектам (*ALLOBJ) и служебными правами доступа (*SERVICE) входить в систему с любой рабочей станции. Разрешив доступ привилегированных пользовательских профайлов только к конкретным хорошо-управляемым рабочим станциям, вы увеличиваете эффективность защиты.

Системное значение QLMTSECOFR применяется только на уровне защиты 30 и выше. В разделе “Рабочие станции” на стр. 211 приведена дополнительная информация о правах доступа, необходимых для входа в систему с рабочей станции.

Значение QLMTSECOFR не ограничивает вход в систему от имени пользовательских профайлов QSECOFR, QSRV и QSRVBAS с помощью консоли.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 12. Для системного значения QLMTSECOFR предусмотрены следующие значения:

1	Пользователь со специальными правами доступа *ALLOBJ или *SERVICE может войти в систему с рабочей станции только в том случае, если ему отдельно предоставлены права доступа к этой рабочей станции (права доступа *CHANGE), либо если пользовательский профайл QSECOFR обладает правами доступа (*CHANGE) к ней. В данном случае недопустимы общие права доступа.
0	Пользователи со специальными правами доступа *ALLOBJ и *SERVICE могут входить в систему с любой рабочей станции, для которой они обладают правами доступа *CHANGE. Права доступа *CHANGE можно получить с помощью частных прав доступа, общих прав доступа, либо специальных прав доступа *ALLOBJ.

Рекомендуемое значение: 1 (Да)

Максимальное число попыток входа в систему (QMAXSIGN)

Системное значение Максимальное число попыток входа в систему (QMAXSIGN) позволяет управлять числом последовательных неудачных попыток в хода в систему локальных и удаленных пользователей.

Вход в систему будет неудачным, если указан неверный ИД пользователя или пароль, либо отсутствуют права доступа к рабочей станции.

Системное значение QMAXSGNACN позволяет определить действие, выполняемое при достижении максимального числа попыток входа в систему или ввода пароля. Для уведомления системного

администратора о возможном вторжении в очередь сообщений QSYSOPR (а также в очередь сообщений QSYSMSG, если она существует в библиотеке QSYS) отправляется соответствующее сообщение CPF1393.

Если вы создадите очередь QSYSMSG в библиотеке QSYS, то сообщения о наиболее важных событиях в системе будут отправляться не только в эту очередь, но и в очередь QSYSOPR. Появление сообщений в очереди QSYSMSG может отслеживаться независимо программой или системным оператором. Такой подход обеспечивает дополнительную защиту ресурсов вашей системы. Из-за того что в очередь QSYSOPR направляется большое число сообщений, некоторые важные сообщения могут остаться незамеченными.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 13. Для системного значения QMAXSIGN предусмотрены следующие значения:

<u>3</u>	Пользователю разрешено максимум три попытки входа в систему или ввода пароля.
*NOMAX	Число попыток входа в систему или ввода пароля не ограничено. В этом случае злоумышленник будет располагать неограниченным числом попыток для подбора правильной комбинации ИД пользователя и пароля.
число	Укажите значение от 1 до 25. Рекомендуемое число попыток входа в систему - 3. Как правило, трех попыток достаточно для исправления ошибок ввода и предотвращения несанкционированного доступа.

Рекомендуемое значение: 3

Действие при достижении максимального числа попыток входа в систему (QMAXSGNACN)

Системное значение QMAXSGNACN (Действие при достижении максимального числа попыток входа в систему) определяет действие, выполняемое при достижении максимального числа попыток входа в систему или ввода пароля с рабочей станции.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 14. Для системного значения QMAXSGNACN предусмотрены следующие значения:

<u>3</u>	Отключение как пользовательского профайла, так и устройства.
1	Отключение устройства.
2	Отключение пользовательского профайла.

При необходимости система выключает устройство. Это происходит только в том случае, если неудачные попытки входа в систему выполнялись с одного устройства. Удачный вход в систему сбрасывает счетчик неудачных попыток входа в систему для устройства.

Для отключения пользовательского профайла в параметре *Состояние* указывается значение *DISABLED. Пользовательский профайл отключается, если число неудачных попыток входа в систему достигает значения, указанного в системном значении QMAXSIGN, независимо от того, выполнялись эти попытки с одного или разных устройств. Удачный вход в систему или ввод правильного пароля сбрасывает счетчик неудачных попыток входа в систему для пользовательского профайла.

Если в библиотеке QSYS создана очередь сообщений QSYSMSG, то в нее отправляется сообщение (CPF1397), в котором указаны имена пользователя и устройства. Такой подход позволяет управлять отключением устройств.

Дополнительная информация об очереди сообщений QSYSMSG приведена в разделе “Максимальное число попыток входа в систему (QMAXSIGN)” на стр. 32.

Если отключен профайл QSECOFR, его можно включить, зарегистрировавшись в системе от имени QSECOFR с помощью консоли. Если консоль выключена и другие пользователи не обладают правами доступа, достаточными для ее включения, необходимо выполнить IPL системы.

Рекомендуемое значение: 3

Сохранить идентификационные данные на сервере (QRETSVRSEC)

Системное значение Сохранить идентификационные данные на сервере (QRETSVRSEC) позволяет определить, следует ли сохранять на хосте зашифрованную идентификационную информацию, связанную с пользовательскими профайлами или записями контрольного списка (*VLDL). Пароли пользовательских профайлов System i в данном случае не сохраняются.

Если изменить значение с 1 на 0, то доступ к идентификационной информации блокируется. Если снова указать значение 1, то доступ к идентификационной информации восстанавливается.

Для удаления идентификационной информации из системы укажите в системном значении QRETSVRSEC значение 0 и выполните команду Очистить данные защиты сервера (CLRSVRSEC). Для обработки большого числа пользовательских профайлов и контрольных списков команда CLRSVRSEC может выполняться в течение длительного времени.

Как правило идентификационная информация хранится в зашифрованном поле данных записи контрольного списка. Приложения указывают необходимость хранения зашифрованных данных в виде, доступном или недоступном для расшифровки. Если приложения выбирают вид доступный для расшифровки и в системном значении QRETSVRSEC указано значение 0, то зашифрованное поле данных становится недоступным. Если зашифрованное поле данных записи контрольного списка хранится в виде недоступном для расшифровки, то системное значение QRETSVRSEC на него не влияет.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 15. Для системного значения QRETSVRSEC предусмотрены следующие значения:

0	Идентификационные данные на сервере не сохраняются.
1	Идентификационные данные сохраняются на сервере.

Рекомендуемое значение: 0

Понятия, связанные с данным

“Работа с контрольными списками” на стр. 256

Контрольные списки позволяют приложениям обеспечить защищенное хранение идентификационной информации пользователей.

Удаленное включение и перезапуск (QRMTIPL)

В плане защиты системы необходимо определить, могут ли удаленные пользователи включать и перезапускать систему. Системное значение Разрешить удаленное включение и перезапуск (QRMTIPL) позволяет запустить удаленную систему с помощью телефона и модема или сигнала SPCN.

Если QRMTIPL равно 1 (Да), то система может быть перезапущена с помощью телефонного звонка. Это системное значение управляет перезапуском, но тем не менее влияет на защиту. Очевидно, что не следует перезапускать систему непредвиденно. Однако, если удаленная система должна администрировать эту систему, то следует разрешить удаленный перезапуск.

Таблица 16. Возможные значения для QRMTIPL

0	Запрет удаленного включения и перезапуска
1	Разрешение удаленного включения и перезапуска

Информация, связанная с данной

Параметры перезапуска системы: Разрешение удаленного включения и перезапуска

Управление удаленным входом в систему (QRMTSIGN)

Системное значение Управление удаленным входом в систему (QRMTSIGN) задает способ обработки запросов на удаленных вход в систему.


Примеры удаленного входа в систему: вход с рабочей станции, подключенной к другой системе, применение на рабочей станции лицензионной программы System i Access и доступ с помощью TELNET.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 17. Для системного значения QRMTSIGN предусмотрены следующие значения:

*FRCSIGNON	Запросы на удаленный вход в систему обрабатываются обычным образом.
*SAMEPRF	Если имена исходного и целевого пользовательских профайлов совпадают и запрошен автоматический вход в систему, то меню входа в систему пропускается. Проверка пароля выполняется до применения целевой программы удаленного входа в систему. Если при попытке автоматического входа в систему указан недопустимый пароль, сеанс удаленного входа в систему завершается и пользователю отправляется сообщение об ошибке. Однако, если имена пользовательских профайлов не совпадают, сеанс завершается с ошибкой защиты даже в том случае, если указан допустимый пароль удаленного пользовательского профайла. Для попыток удаленного входа в систему, не запрашивающих автоматический вход, отображается меню входа в систему.
*VERIFY	Значение *VERIFY позволяет пропустить меню входа в целевую систему, если вместе с запросом на автоматический вход в систему отправляется допустимая идентификационная информация. Если для указанного целевого пользовательского профайла введен недопустимый пароль, сеанс удаленного входа в систему завершается с ошибкой защиты. На уровне защиты 10 (QSECURITY) разрешены все запросы на автоматический вход в систему. Для попыток удаленного входа в систему, не запрашивающих автоматический вход, отображается меню входа в систему.
*REJECT	Удаленный вход в систему не разрешен. Для TELNET действие для значения *REJECT отсутствует.
<i>имя-программы имя-библиотеки</i>	В начале и конце всех сеансов удаленного входа в систему выполняется указанная программа.

Рекомендуемое значение: *REJECT, позволяет запретить удаленный доступ к системе и System i Access. Для разрешения удаленного доступа к системе или System i Access рекомендуется применять значения *FRCSIGNON и *SAMEPRF.

В книге Remote Workstation Support  приведена подробная информация о системном значении QRMTSIGN. Кроме того, в ней перечислены требования к программе удаленного входа в систему и приведен ее пример.

Сканирование в файловых системах (QSCANFS)

Системное значение Сканирование в файловых системах (QSCANFS) позволяет указать интегрированные файловые системы для сканирования объектов.

Например, с помощью этой опции можно выполнить поиск вирусов. Сканирование в интегрированной файловой системе применяется в случае регистрации программ выхода с точками выхода, связанными со сканированием интегрированных файловых систем. Системное значение QSCANFS задает файловые системы, в которых должно выполняться сканирование объектов в случае регистрации программ выхода с точками выхода, связанными со сканированием интегрированных файловых систем.

Ниже перечислены точки выхода, связанные со сканированием интегрированных файловых систем:

- QIBM_QP0L_SCAN_OPEN — Сканирование в интегрированной файловой системе при открытии программы выхода.
- QIBM_QP0L_SCAN_CLOSE — Сканирование в интегрированной файловой системе при закрытии программы выхода.

Дополнительная информация об интегрированных файловых системах приведена в разделе Интегрированная файловая система.

Таблица 18. Для системного значения QSCANFS предусмотрены следующие значения:

*NONE	Сканирование объектов в интегрированных системах не выполняется.
*ROOTPNUD	Выполняется сканирование объектов типа *STMF, расположенных в каталогах *TYPE2 корневой (/) и пользовательских файловых систем и файловой системы QOpenSys.

Рекомендуемое значение: *ROOTPNUD. Это значение позволяет выполнить сканирование в корневой (/) и пользовательских файловых системах и файловой системе QOpenSys и в случае регистрации программ выхода с точками выхода, связанными со сканированием в интегрированной файловой системе.

Ссылки, связанные с данной

“Управление сканированием в файловых системах (QSCANFSCTL)”

Системное значение Управление сканированием в файловых системах (QSCANFSCTL) управляет процессом сканирования в интегрированных файловых системах, которое применяется в случае регистрации программ выхода с точками выхода, связанными со сканированием в интегрированной файловой системе.

Информация, связанная с данной

Каталоги *TYPE2

Управление сканированием в файловых системах (QSCANFSCTL)

Системное значение Управление сканированием в файловых системах (QSCANFSCTL) управляет процессом сканирования в интегрированных файловых системах, которое применяется в случае регистрации программ выхода с точками выхода, связанными со сканированием в интегрированной файловой системе.

QSCANFSCTL работает с системным значением сканирования в файловых системах и обеспечивает возможность тонкого управления сканированием в интегрированной файловой системе. Можно применять

параметры сканирования по умолчанию или настроить другие параметры. Также можно указать опции сканирования, управляющие объектами и способом сканирования с помощью зарегистрированной программы выхода. Эти опции описаны в следующей таблице:

Таблица 19. Для системного значения QSCANFCTL предусмотрены следующие значения:

*NONE	Точки выхода, связанные со сканированием в интегрированной файловой системе, не управляются:
*ERRFAIL	Если при вызове программы выходе происходят ошибки (например, не удалось найти программу или программа выхода обнаружила ошибку), система не выполнит запрос, вызвавший программу выхода. Если это значение не указано, программа выхода пропускается и считается, что объект не сканировался.
*FSVRONLY	Сканирование выполняется только для обращений с помощью файловых серверов. Например, сканирование будет выполнено для обращений с помощью сетевой файловой системы и других методов, применяющих файловые серверы. Если это значение не указано, сканируются все обращения.
*NOFAILCLO	Запросы на закрытие с указанием на ошибку сканирования выполняются даже в том случае, если в процессе закрытия не удалось выполнить сканирование объекта. Кроме того, для данной точки выхода, связанной со сканированием, это значение переопределяет спецификацию обработки закрытия *ERRFAIL.
*NOPOSTRST	<p>После восстановления объектов сканирование не выполняется. Если для объекта указан атрибут "не сканировать объект", то сканирование объекта запрещено. Если для объекта указан атрибут "сканировать объект только в случае внесения в него изменений с момента последнего сканирования", то сканирование объекта выполняется только в том случае, если после восстановления он был изменен.</p> <p>Если значение *NOPOSTRST не указано, то после восстановления сканирование объектов выполняется по крайней мере один раз. Если для объекта указан атрибут "не сканировать объект", то сканирование объекта будет выполнено один раз после восстановления. Если для объекта указан атрибут "сканировать объект только в случае внесения в него изменений с момента последнего сканирования", то после восстановления объект будет отсканирован, так как в этом случае восстановление рассматривается как изменение объекта.</p> <p>Как правило восстановление объектов без сканирования связано с определенным риском. Рекомендуется указывать эту опцию, если вы уверены, что перед сохранением объектов было выполнено их сканирование, либо они получены из надежного источника.</p>
*NOWRTUPG	Система не пытается добавить права доступа на запись к дескриптору сканирования, передаваемому программе выхода. Если это значение не указано, система попытается добавить права доступа на запись.
*USEOCOATR	Применяется спецификация атрибута "только изменение объекта" для сканирования измененного объекта (обновления, обнаруженные программным обеспечением сканирования, не учитываются). Если это значение не указано, то атрибут "только изменение объекта" не применяется и сканирование выполняется после изменения объекта, либо в случае обнаружения его обновления программным обеспечением сканирования.

Рекомендуемое значение: Для наиболее жесткого ограничения сканирования в интегрированной файловой системе рекомендуется указать значения *ERRFAIL и *NOWRTUPG. Это позволяет запретить связанные операции программы выхода сканирования, в которой произошел сбой, а также не предоставлять программе выхода дополнительных прав доступа. Однако для большинства пользователей рекомендуется указывать опцию *NONE. На время установки программного обеспечения, полученного из надежного источника, рекомендуется указать значение *NOPOSTRST.

Ссылки, связанные с данной

“Сканирование в файловых системах (QSCANFS)” на стр. 36

Системное значение Сканирование в файловых системах (QSCANFS) позволяет указать интегрированные файловые системы для сканирования объектов.

Управление общей памятью (QSHRMEMCTL)

Системное значение Управление общей памятью (QSHRMEMCTL) определяет пользователей, которым разрешено работать с общей памятью и памятью прямого доступа с возможностью записи.

Ваша среда может содержать приложения, выполняющие разные задания, но применяющие общие адреса в памяти. Эти API улучшают быстродействие приложений и упрощают разработку приложений с применением общей памяти и потоковых файлов. Однако эти API могут представлять угрозу для защиты системы и ресурсов. Программист может предоставить права доступа на запись к объектам в общей памяти и потоковым файлам, и может тем самым добавить, изменить или удалить записи.

Для изменения этого системного значения требуются специальные права доступа *ALLOBJ и *SECADM. Изменения, внесенные в это системное значение, вступают в силу немедленно.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 20. Для системного значения QSHRMEMCTL предусмотрены следующие значения:

0	<p>Пользователям запрещено работать с общей памятью и памятью прямого доступа с возможностью записи.</p> <p>Это значение означает, что пользователи не могут работать с API общей памяти (например, shmat() - API Добавление общей памяти), а также не могут работать с объектами прямого доступа с возможностью записи (например, mmap() - API Прямой доступ к файлу).</p> <p>Это значение рекомендуется применять в средах с высокими требованиями к защите.</p>
1	<p>Пользователи могут работать с общей памятью и памятью прямого доступа с возможностью записи.</p> <p>Это значение означает, что пользователям разрешено работать с API общей памяти (например, shmat() - API Добавление общей памяти), а также с объектами прямого доступа с возможностью записи (например, mmap() - API Прямой доступ к файлу).</p>

Рекомендуемое значение: 1

Применять принятые права доступа (QUSEADPAUT)

Системное значение Применять принятые права доступа (QUSEADPAUT) определяет пользователей, которым разрешено создавать программы с атрибутом Применять принятые права доступа (*USEADPAUT(*YES)).

Все пользователи, указанные с помощью системного значения QUSEADPAUT, могут создавать и изменять программы и служебные программы, позволяющие пользователям обладающим к ним доступом, использовать принятые права доступа.

В системном значении можно указать имя списка прав доступа. Права доступа пользователя проверяются в соответствии с этим списком. Если пользователь обладает по крайней мере правами доступа *USE к этому списку прав доступа, то он может создавать, изменять и обновлять программы и служебные программы с атрибутом USEADPAUT(*YES). Права доступа к списку прав доступа могут быть предоставлены с помощью принятых прав доступа.

Если список прав доступа, указанный в системном значении, не существует, то запрашиваемая функция выполнена не будет. При этом выдается соответствующее сообщение.

Однако, если программа создается с помощью API QPRCRTPG и в шаблоне опций указано значение *NOADPAUT, то программа будет создана успешно даже в том случае, если список прав доступа не существует.

Если список прав доступа не существует, то все функции, запрашиваемые в команде или API, не выполняются.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 21. Для системного значения QUSEADPAUT предусмотрены следующие значения:

имя списка прав доступа	Для уведомления о создании программы с USEADPAUT(*NO) выдается диагностическое сообщение, если выполняются все следующие условия: <ul style="list-style-type: none"> • У пользователя нет прав доступа к указанному списку прав доступа. • При создании программы или служебной программы другие ошибки не происходили.
*NONE ¹	Все пользователи могут создавать, обновлять и изменять программы и служебные программы, позволяющие пользователям обладающим правами доступа к ним, использовать принятые права доступа.
¹ *NONE указывает, что список прав доступа не применяется, и по умолчанию все пользователи будут иметь доступ к программам, применяющим принятые права доступа.	

Рекомендуемое значение: Для рабочих систем рекомендуется создавать списки прав доступа с правами доступа *PUBLIC(*EXCLUDE). Укажите в системном значении QUSEADPAUT такой список прав доступа. Это позволит запретить создание программ, использующих принятые права доступа.

Перед созданием списка прав доступа для системного значения QUSEADPAUT рекомендуется тщательно спланировать структуру защиты приложения. В особенности это важно для сред разработки приложений.

Системные значения, связанные с защитой

В этом разделе описаны системные значения, связанные с защитой операционной системы i5/OS.

Описание:

Задача:

Системные значения, связанные с защитой системы.

Средства для ее решения:

WRKSYSVAL (команда Работа с системными значениями)

Права доступа:

*ALLOBJ и *SECADM

Запись в журнале:

SV

Прим.: Изменения вступают в силу немедленно. IPL не требуется.

Ниже приведено описание дополнительных системных значений, связанных с защитой системы. Эти системные значения не включены в группу *SEC меню Работа с системными значениями.

QAUTOCFG

Автоматическая настройка устройств

QAUTOVRT

Автоматическая настройка виртуальных устройств

QDEVRCYACN

Действие по восстановлению устройства

QDSCJOBTV

Тайм-аут для отключенного задания

Примечание: Описание этого системного значения также приведено в разделе Системные значения для работы с заданиями: Тайм-аут отсоединенных заданий.

QRMTSRVATR

Атрибут удаленной службы

QSSLCSL

Список шифров Secure Sockets Layer (SSL)

QSSLCSLCTL

Управление шифрами Secure Sockets Layer (SSL)

QSSLPCL

Протоколы Secure Sockets Layer (SSL)

Понятия, связанные с данным

“Проверка восстанавливаемых программ” на стр. 18

При создании программы система вычисляет контрольное значение, которое сохраняется вместе с программой. В процессе восстановления программы контрольное значение вычисляется вновь и сравнивается в контрольным значением, сохраненным с программой.

Автоматическая настройка устройств (QAUTOCFG)

Системное значение Автоматическая настройка устройств (QAUTOCFG) предназначено для автоматической настройки локально подключенных устройств. Это значение позволяет указать необходимость автоматической настройки устройств, добавляемых в систему.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 22. Для системного значения QAUTOCFG предусмотрены следующие значения:

0	Автоматическая настройка не выполняется. Локальные контроллеры и устройства, добавляемые в систему, должны настраиваться вручную.
1	Автоматическая настройка выполняется. Локальные контроллеры и устройства, добавляемые в систему, настраиваются автоматически. В случае изменения конфигурации системы оператор получает соответствующее сообщение.

Рекомендуемое значение: Значение 1 должны быть указано в процессе начальной настройки системы, а также в случае добавления большого числа новых устройств. В остальных случаях должно быть указано значение 0.

Автоматическая настройка виртуальных устройств (QAUTOVRT)

Системное значение Автоматическая настройка виртуальных устройств (QAUTOVRT) задает необходимость автоматической настройки виртуальных устройств удаленного входа в систему и виртуальных устройств полноэкранного TELNET (вместо виртуального устройства функции рабочей станции).

Виртуальное устройство представляет собой описание устройства, с которым не связано аппаратное обеспечение. Они применяются для создания соединения между пользователем и физической рабочей станцией, подключенной к удаленной системе.

Возможность автоматической настройки виртуальных устройств облегчает для пользователей процедуру удаленного входа в систему, а также работу с telnet. Если автоматическая настройка не применяется, то число попыток входа в систему с помощью виртуальных устройств ограничено. Ограничение определяется системным администратором с помощью системного значения QMAXSIGN. Применение автоматической настройки позволяет увеличить фактическое ограничение. Ограничение на число попыток входа в систему умножается на число виртуальных устройств, которые можно создать с помощью функций поддержки автоматической настройки. Данная поддержка определяется в системном значении QAUTOVRT.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 23. Для системного значения QAUTOVRT предусмотрены следующие значения:

0	Автоматическое создание виртуальных устройств запрещено.
<i>число- виртуальных- устройств</i>	Укажите значение от 1 до 9999. Система настраивает новое устройство каждый раз при получении запроса на удаленный вход в систему или запуск полноэкранного TELNET, если доступные виртуальные устройства отсутствуют. Для этого число устройств, подключенных к виртуальному контроллеру, не должно превышать указанное в этом системном значении.

Рекомендуемое значение: 0

Информация, связанная с данной



Поддержка удаленных рабочих станций

Настройка TCP/IP

Действие по восстановлению устройства (QDEVRCYACN)

Системное значение Действие по восстановлению устройства (QDEVRCYACN) задает действие, выполняемое в случае возникновения ошибок ввода-вывода в рабочей станции интерактивного задания.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 24. Для системного значения QDEVRCYACN предусмотрены следующие значения:

*DSCMSG	Отключает задание. Повторный вход в систему приводит к отправке прикладной программе пользователя сообщения об ошибке.
*MSG	Отправляет прикладной программе пользователя сообщение об ошибке ввода-вывода. Прикладная программа выполняет восстановление.
*DSCENDRQS	Отключает задание. Повторный вход в систему приводит к отмене запроса. Контроль над заданием возвращается последнему уровню запроса.
*ENDJOB	Задание завершается. Для задания создается протокол задания. В протокол задания и протокол QHST заносится сообщение, указывающее на завершение задания вследствие ошибки устройства. Для того чтобы максимально снизить воздействие завершения задания на производительность системы выполняются следующие действия: приоритет задания понижается до 10, для кванта времени задается значение 100 миллисекунд и для атрибута очистки указывается значение Да.

Таблица 24. Для системного значения QDEVRCYACN предусмотрены следующие значения: (продолжение)

*ENDJOBNO LIST	Задание завершается. Для задания не создается протокол задания. В протокол QHST заносится сообщение, указывающее на завершение задания вследствие ошибки устройства.
----------------	--

Если указано значение *MSG или *DSCMSG, то действие по восстановлению устройства выполняется только после выполнения заданием следующей операции ввода-вывода. В среде LAN/WAN перед выполнением следующей операции ввода-вывода к этому же адресу может подключиться другое устройство. Задание может быть восстановлено после получения сообщения об ошибке ввода-вывода и продолжить работу со вторым устройством. Для того чтобы избежать этого, укажите значение *DSCENDRQS, *ENDJOB или *ENDJOBNO LIST. Данные действия по восстановлению устройства выполняются немедленно после возникновения ошибки ввода-вывода, такой как операция выключения.

Рекомендуемое значение: *DSCMSG

Примечание: Для изменения этого значения не требуются специальные права доступа *ALLOBJ и *SECADM.

Тайм-аут для отключенного задания (QDSCJOBITV)

Системное значение Тайм-аут для отключенного задания (QDSCJOBITV) определяет необходимость завершения отключенного задания, а также время, через которое его необходимо отключить. Время указывается в минутах.

Если в системном значении QINACTMSGQ указано, что неактивные задания должны отключаться (*DSCJOB), то в QDSCJOBITV следует указать завершение отключенных заданий. Отключенное задание использует системные ресурсы, а также блокирует объекты.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 25. Для системного значения QDSCJOBITV предусмотрены следующие значения:

240	Система завершает отключенное задание через 240 минут.
*NONE	Отключенные задания автоматически не завершаются.
<i>время-в-минутах</i>	Укажите значение от 5 до 1440.

Рекомендуемое значение: 120

Атрибут удаленного обслуживания (QRMTSRVATR)

Атрибут удаленного обслуживания (QRMTSRVATR) позволяет управлять функциями анализа неполадок удаленного обслуживания. С помощью этого значения можно выполнить удаленный анализ системы.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Для системного значения QRMTSRVATR предусмотрены следующие значения:

Таблица 26. Для системного значения QRMTSRVATR предусмотрены следующие значения:

0	Атрибут удаленного обслуживания отключен.
1	Атрибут удаленного обслуживания включен.

Рекомендуемое значение: 0

Понятия, связанные с данным

“Защита с помощью ключа” на стр. 2

Получить или изменить позицию ключа можно с помощью API Получить атрибуты IPL (QWCRIPLA) или команды Изменить атрибуты IPL (CHGIPLA).

Список шифров Secure Sockets Layer (SSL) (QSSLCSL)

Системное значение Список шифров Secure Sockets Layer (SSL) (QSSLCSL) указывает, какие шифры поддерживаются системными функциями SSL.

Функции SSL системы используют значения QSSLCSL для упорядочения списка шифров SSL в системе. Записи списка шифров по умолчанию задаются системой и могут изменяться в новых выпусках. Если из системного значения QSSLCSL удаляется комплект шифров по умолчанию, то он также удаляется из списка шифров по умолчанию. При добавлении в системное значение QSSLCSL комплекта шифров по умолчанию он также добавляется в список шифров по умолчанию. В список шифров по умолчанию нельзя добавлять другие комплекты шифров, помимо заданных в данном выпуске системы. Кроме того, комплект шифров невозможно добавить в QSSLCSL, если обязательный протокол SSL не задан для системного значения QSSLPCL (список протоколов SSL).

Значения QSSLCSL доступны только для чтения, если системное значение Управление шифрами SSL (QSSLCSLCTL) не равно *USRDFN.

Для системного значения QSSLCSL предусмотрены следующие значения:

- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_NULL_SHA
- *RSA_NULL_MD5
- *RSA_RC2_CBC_128_MD5
- *RSA_3DES_EDE_CBC_MD5
- *RSA_DES_CBC_MD5

Примечание: Для изменения этого системного значения необходимы специальные права доступа *IOSYSCFG, *ALLOBJ и *SECADM.

Дополнительная информация о поставляемых значениях приведена в разделе об списке шифров SSL публикации Системные значения.

Информация, связанная с данной

Параметры защиты системы: список шифров Secure Sockets Layer

Системные свойства SSL

Управление шифрами Secure Sockets Layer (SSL) (QSSLCSLCTL)

Системное значение Управление шифрами Secure Sockets Layer (SSL) (QSSLCSLCTL) указывает, кто управляет системным значением Список шифров Secure Sockets Layer (SSL) (QSSLCSL), система или пользователь.

| Для системного значения QSSLCSLCTL предусмотрены следующие значения:

- | • *OPSYS
- | • *USRDFN

| **Примечание:** Для изменения этого системного значения необходимы специальные права доступа *IOSYSCFG, *ALLOBJ и *SECADM.

| Дополнительная информация о поставляемых значениях приведена в разделе об управлении шифрами SSL публикации Системные значения.

| **Информация, связанная с данной**

| Параметры защиты системы: управление шифрами Secure Sockets Layer

| **Протоколы Secure Sockets Layer (SSL) (QSSLPCL)**

| Системное значение Протоколы Secure Sockets Layer (SSL) (QSSLPCL) указывает, какие протоколы SSL поддерживаются системными функциями.

| Для системного значения QSSLPCL предусмотрены следующие значения:

- | • *OPSYS
- | • *TLSV1
- | • *SSLV2
- | • *SSLV3

| **Примечание:** Для изменения этого системного значения необходимы специальные права доступа *IOSYSCFG, *ALLOBJ и *SECADM.

| Дополнительная информация о поставляемых значениях приведена в разделе о протоколах SSL публикации Системные значения.

| **Информация, связанная с данной**

| Параметры защиты системы: протоколы Secure Sockets Layer

Системные значения восстановления, связанные с защитой

В этом разделе описаны системные значения, связанные с восстановлением операционной системы i5/OS.

Описание:

Задача:

Управляет восстановлением объектов, связанных с защитой.

Средства для ее решения:

WRKSYSVAL *SEC (команда Работа с системными значениями)

Права доступа:

*ALLOBJ и *SECADM

Запись в журнале:

SV

Прим.: Изменения вступают в силу немедленно. IPL не требуется.

Ниже приведено описание системных значений, применяемых для восстановления объектов, связанных с защитой. Дополнительная информация о системном значении QSCANFSCCTL *NOPOSTRST приведена в разделе Табл. 19 на стр. 37.

QVIFYOBJRST

Проверять восстанавливаемые объекты

QFRCCVNRST

Преобразование при восстановлении

QALWOBJRST

Разрешить восстановление конфиденциальных объектов

Описание этих системных значений приведено ниже. Для каждого системного значения указаны возможные значения. Подчеркнутые значения являются системными значениями по умолчанию.

Понятия, связанные с данным

“Восстановление программ” на стр. 266

Восстановление в системе программ, полученных из неизвестного источника, представляет собой потенциальную опасность. В этом разделе приведена информация об особенностях восстановления программ.

Проверять восстанавливаемые объекты (QVFYOBJRST)

Системное значение Проверять восстанавливаемые объекты (QVFYOBJRST) позволяет запретить восстановление объектов без цифровых подписей.

В этом случае для восстановления объекта потребуется цифровая подпись от надежного поставщика программного обеспечения. Это значение применимо для объектов следующих типов: *PGM, *SRVPGM, *SQLPKG, *CMD и *MODULE. Кроме того, оно применимо к объектам *STMF, содержащим программы Java.

Запрос на восстановление объекта проверяется с помощью трех системных значений, выполняющих роль фильтров. Первый фильтр представляет собой системное значение Проверять восстанавливаемые объекты (QVFYOBJRST). Оно управляет процессом восстановления объектов с электронной подписью. Второй фильтр - это системное значение Преобразование при восстановлении (QFRCCVNRST). Это системное значение позволяет указать необходимость преобразования программ, служебных программ, пакетов SQL и объектов модулей в процессе восстановления. Кроме того, оно запрещает восстановление некоторых объектов. Третий фильтр обрабатывает только те объекты, которые прошли проверку первых двух. Третьим фильтром является системное значение Разрешить восстановление объектов (QALWOBJRST). Оно указывает, разрешается ли восстанавливать объекты с конфиденциальными атрибутами.

Если в системе не установлен Диспетчер цифровых сертификатов (i5/OS, опция 34), то в процессе восстановления все объекты, за исключением объектов, подписанных надежным источником, обрабатываются с помощью системного значения QVFYOBJRST как неподписанные.

| Программа, служебная программа и объекты модулей, созданные или преобразованные в системе выпуска
| до V6R1, считаются неподписанными, если восстановление выполняется в системе V6R1 или более поздней.
| Аналогично, программа, служебная программа и объекты модулей, созданные или преобразованные в
| системе V6R1 или более поздней, считаются неподписанными, если восстановление выполняется в системе
| версии более ранней, чем V6R1.

Изменения, внесенные в это системное значение, вступают в силу немедленно.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.
2. Объекты с атрибутами режима системы и атрибутами режима наследования должны быть подписаны надежным источником. Объекты в PTF Лицензионного внутреннего кода также должны быть подписаны надежным источником. Если объект не имеет правильной подписи, то восстановление его невозможно независимо от системного значения QVFYOBJRST.

Внимание: Во время поставки системы в QVFYOBJRST указано значение 3. Для установки нового выпуска операционной системы i5/OS значение системного значения QVFYOBJRST не должно превышать 3.

Таблица 27. Для системного значения QVFYOBJRST предусмотрены следующие значения:

1	<p>При восстановлении подписи не проверяются. Восстанавливаются все пользовательские объекты независимо от их подписей.</p> <p>Это значение следует применять только в том случае, если необходимо восстановить объекты, проверка подписей которых не может быть выполнена успешно.</p>
2	<p>Проверять объекты при восстановлении. Восстанавливаются неподписанные команды и объекты режима пользователя. Восстанавливаются подписанные команды и объекты режима пользователя с недопустимыми подписями.</p> <p>Используйте это значение только для восстановления объектов с неправильной подписью. Как правило, восстановление объектов с недопустимыми подписями не рекомендуется.</p>
3	<p>При восстановлении подписи проверяются. Восстанавливаются неподписанные команды и объекты режима пользователя. Восстанавливаются подписанные команды и объекты режима пользователя с допустимыми подписями.</p> <p>Это значение рекомендуется для обычной работы, если некоторые из восстанавливаемых объектов могут быть не подписаны, но необходимо устанавливать только подписанные объекты с допустимыми подписями. Это значение позволяет восстанавливать команды и программы, созданные или приобретенные до того, как цифровые подписи стали доступны. Это значение по умолчанию.</p>
4	<p>При восстановлении подписи проверяются. Неподписанные команды и объекты режима пользователя не восстанавливаются. Восстанавливаются подписанные команды и объекты режима пользователя с недопустимыми подписями.</p> <p>Используйте это значение только для восстановления объектов с неправильной подписью, если при этом требуется не включать возможность восстановления неподписанных объектов. Как правило, восстановление объектов с недопустимыми подписями не рекомендуется.</p>
5	<p>При восстановлении подписи проверяются. Неподписанные команды и объекты режима пользователя не восстанавливаются. Восстанавливаются подписанные команды и объекты режима пользователя с допустимыми подписями.</p> <p>Это значение накладывает самые жесткие ограничения. Его рекомендуется применять для восстановления подписанных объектов из надежных источников.</p>

Некоторые команды применяют подписи, защищающие не все части объектов. Некоторые части команды не подписываются, тогда как другие подписываются только в том случае, если в них указано ненулевое значение. Подписи такого типа позволяют вносить изменения в объекты без аннулирования подписи. Примеры изменений, не аннулирующих подписи такого типа:

- Изменение значений команды по умолчанию.
- Добавление программы проверки правильности данных в команду, не содержащую такой программы.
- Изменение значения параметра Где разрешено запускать.
- Изменение параметра "разрешить пользователя с ограниченными возможностями".

При необходимости вы можете добавить в эти объекты подписи, защищающие данные области.

Рекомендуемое значение: 3

Преобразование при восстановлении (QFRCCVNRST)

Системное значение Преобразование при восстановлении (QFRCCVNRST) предназначено для принудительного преобразования некоторых типов объектов при восстановлении. Кроме того, оно запрещает восстановление некоторых объектов.

Системное значение QFRCCVNRST позволяет указать необходимость преобразования в процессе восстановления объектов следующих типов:

- программа (*PGM)
- служебная программа (*SRVPGM)
- Пакет SQL (*SQLPKG)
- модуль (*MODULE)

Если для преобразования объекта, указанного в системном значении, недостаточно данных о создании, то восстановление не выполняется.

Значение этого системного значения применяется в командах восстановления (RST, RSTLIB, RSTOBJ, RSTLICPGM), в параметре FRCOBJCVN которых указано значение *SYSVAL. Поэтому изменив значение QFRCCVNRST вы можете включить или выключить преобразование во всей системе. Однако в некоторых случаях это системное значение переопределяется параметром FRCOBJCVN. Указав для параметра FRCOBJCVN значения *YES и *ALL, вы переопределите все параметры системного значения QFRCCVNRST. Если для параметра FRCOBJCVN указаны значения *YES и *RQD, они соответствуют значению '2' этого системного значения и переопределяют значения 0 и 1.

Системное значение QFRCCVNRST представляет собой второе из трех системных значений, выполняющих роль фильтров, которые определяют, разрешено ли восстановление объекта или в процессе восстановления следует его преобразовать. Первый фильтр, Проверять восстанавливаемые объекты (QVFYOBJRST), управляет восстановлением подписанных объектов. Третий фильтр обрабатывает только те объекты, которые прошли проверку первых двух. Системное значение Разрешить восстановление объектов (QALWBJRST) позволяет разрешить или запретить восстановление объектов с конфиденциальными атрибутами.

| Если в системе не установлен Диспетчер цифровых сертификатов (i5/OS компонент 34), то в процессе восстановления все объекты, за исключением объектов, подписанных надежным источником, обрабатываются с помощью системного значения QFRCCVNRST как неподписанные.

| Программа, служебная программа и объекты модулей, созданные или преобразованные в системе выпуска до V6R1, считаются неподписанными, если восстановление выполняется в системе V6R1 или более поздней. Аналогично, программа, служебная программа и объекты модулей, созданные или преобразованные в системе V6R1 или более поздней, считаются неподписанными, если восстановление выполняется в системе версии более ранней, чем V6R1.

Поставляемое значение QFRCCVNRST - 1. Для всех значений QFRCCVNRST восстановление объектов, преобразование которых невозможно, не выполняется. Объекты, подписанные надежным источником, всегда восстанавливаются без преобразования.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

В следующей таблице приведены разрешенные значения системного значения QFRCCVNRST:

Таблица 28. Значения QFRCCVNRST

0	Не преобразовывать объекты. Разрешено восстановление всех объектов.
1	Преобразовываются объекты с ошибками проверки данных.

Таблица 28. Значения QFRCCVNRST (продолжение)

2	Преобразовываются объекты с ошибками проверки данных, а также объекты, указанные текущей операционной системой или текущей системой.
3	Преобразуются объекты с возможными повреждениями, с ошибками проверки данных, а также объекты, указанные текущей операционной системой или текущей системой.
4	Преобразуются объекты без допустимых цифровых подписей, если в них содержатся достаточные данные о создании. В противном случае объект восстанавливается без преобразования. Примечание: Для восстановления должны быть преобразованы все объекты (подписанные и неподписанные) с возможными повреждениями, ошибками проверки данных, а также объекты, указанные текущей операционной системой или текущей системой.
5	Преобразуются объекты, содержащие достаточные данные о создании. В противном случае объект восстанавливается без преобразования. Примечание: Для восстановления должны быть преобразованы все объекты с возможными повреждениями, ошибками проверки данных, а также объекты, указанные текущей операционной системой или текущей системой.
6	Преобразуются все объекты, у которых отсутствует допустимая цифровая подпись. Примечание: Объекты с допустимой цифровой подписью и возможными повреждениями или ошибками проверки данных восстанавливаются только в том случае, если они успешно преобразованы.
7	Преобразуются все объекты.
<p>После преобразования объекта его цифровая подпись аннулируется. Преобразованные объекты находятся в режиме пользователя. После преобразования объекты обладают действительным контрольным значением и не считаются поврежденными.</p>	

Рекомендуемое значение: 3 или выше

Разрешить восстановление конфиденциальных значений (QALWOBJRST)

Системное значение Разрешить восстановление конфиденциальных значений (QALWOBJRST) позволяет разрешить или запретить восстановление конфиденциальных объектов.

Запрос на восстановление объекта проверяется с помощью трех системных значений, выполняющих роль фильтров, которые определяют, разрешено ли восстановление объекта или в процессе восстановления следует его преобразовать. Первый фильтр представляет собой системное значение Проверять восстанавливаемые объекты (QVFYOBJRST). Оно управляет процессом восстановления объектов с электронной подписью. Второй фильтр - это системное значение Преобразование при восстановлении (QFRCCVNRST). Это системное значение позволяет указать необходимость преобразования программ, служебных программ, пакетов SQL и объектов модулей в процессе восстановления. Кроме того, оно запрещает восстановление некоторых объектов. Третий фильтр обрабатывает только те объекты, которые прошли проверку первых двух. Третьим фильтром является системное значение Разрешить восстановление объектов (QALWOBJRST). Оно указывает, разрешается ли восстанавливать объекты с конфиденциальными атрибутами. С его помощью можно запретить восстановление объектов режима системы и объектов, принимающих права доступа.

Проставляемое значение системного значения QALWOBJRST равно *ALL. Это значение необходимо для успешной установки системы.

ВНИМАНИЕ: Для выполнения некоторых действий необходимо установить системное значение QALWOBJRST равным *ALL, например:

- Установка нового выпуска лицензионной программы i5/OS.
- Установка лицензионных программ.
- Восстановление системы.

В противном случае эти операции могут быть не выполнены. После завершения системных операций восстановите обычное значение QALWOBJRST. Это необходимо для обеспечения защиты системы.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

В системном значении QALWOBJRST можно указать несколько значений, если в нем не указаны значения *ALL или *NONE.

Таблица 29. Для системного значения QALWOBJRST предусмотрены следующие значения:

*ALL	Пользователь с соответствующими правами доступа может восстановить любой объект.
*NONE	Конфиденциальные объекты, такие как программы режима системы и программы, принимающие права доступа, восстанавливать запрещено.
*ALWSYSSTT	Разрешено восстанавливать объекты режима системы и наследования.
*ALWPGMADP	Разрешено восстановление объектов с принятыми правами доступа в системе.
*ALWPTF	В процессе установки PTF разрешено восстанавливать объекты режима системы и наследования, объекты, принимающие права доступа, а также объекты, для которых указан атрибут S_ISUID(ИД-пользователя) или S_ISGID (ИД-группы).
*ALWSETUID	Разрешено восстанавливать файлы, для которых указан атрибут S_ISUID (ИД-пользователя).
*ALWSETGID	Разрешено восстанавливать файлы, для которых указан атрибут S_ISGID (ИД-группы).
*ALWVLDERR	Разрешено восстановление объектов, не прошедших проверку. Преобразование объекта, выполняемое в соответствии с системным значением QFRCCVNRST, позволяет исправить ошибки проверки.

Рекомендуемое значение: Системное значение QALWOBJRST позволяет защитить систему от программ, которые могут вызвать серьезные неполадки. Для обычной работы рекомендуется выбрать значение *NONE. Перед выполнением операций, перечисленных выше, всегда изменяйте значение на *ALL. Для регулярного восстановления программ и приложений может потребоваться указать в системном значении QALWOBJRST значение *ALWPGMADP.

Системные значения, связанные с паролями

В этом разделе описаны системные значения, связанные с паролями. Эти системные значения позволяют изменять пароли пользователей с указанной частотой, а также избежать выбора простых паролей, которые можно легко угадать. Кроме того, они обеспечивают соответствие паролей с требованиями сети.

Описание:

Задача:

Системные значения, позволяющие задать требования к паролям, которые выбирают пользователи.

Средства для ее решения:

WRKSYSVAL *SEC (команда Работа с системными значениями)

Права доступа:

*ALLOBJ и *SECADM

Запись в журнале:

SV

Прим.: Изменения вступают в силу немедленно (кроме относящихся к QPWDLVL). IPL не требуется.

Системные значения, управляющие паролями:

- | **QPWDCHGBLK**
| Блокировка изменения пароля
- | **QPWDEXPIV**
| Срок действия
- | **QPWDEXPWRN**
| Предупреждение об истечении срока действия пароля
- | **QPWDLVL**
| Уровень пароля
- | **QPWDLMTCHR**
| Запрещенные символы
- | **QPWDLMTAJC**
| Запретить применение последовательности цифр
- | **QPWDLMTREP**
| Запретить повторяющиеся символы
- | **QPWDMINLEN**
| Минимальная длина
- | **QPWDMAXLEN**
| Максимальная длина
- | **QPWDPOSDIF**
| Запретить символы в одинаковых позициях
- | **QPWDRQDDIF**
| Обязательное изменение пароля
- | **QPWDRQDDGT**
| Обязательный числовой символ
- | **QPWDRULES**
| Правила для паролей
- | **QPWDVLDPGM**
| Программа проверки пароля

Системные значения, связанные с составом пароля, применяются только в случае изменения пароля с помощью команды CHGPWD, опции меню Поддержка или API QSYCHGPW. Они не применяются при задании пароля с помощью команд CRTUSRPRF или CHGUSRPRF.

- | Система не разрешит указать с помощью команды CHGPWD, опции меню Поддержка или API QSYCHGPW
- | пароль, совпадающий с именем пользовательского профайла, если выполнено одно из следующих условий.
- | • Системное значение Правила паролей (QPWDRULES) равно *PWDSYSVAL и системное значение
- | Минимальная длина пароля (QPWDMINLEN) не равно 1.
- | • Системное значение Правила паролей (QPWDRULES) равно *PWDSYSVAL и системное значение
- | Максимальная длина пароля (QPWDMAXLEN) не равно 10.

- Системное значение Правила паролей (QPWDRULES) равно *PWDSYSVAL, а любое из прочих системных значений, связанных с паролями, отличается от значения по умолчанию.

Если пользователь забыл пароль, системный администратор с помощью команды Изменить пользовательский профайл (CHGUSRPRF) может задать пароль, совпадающий с именем пользовательского профайла. С помощью поля пользовательского профайла Ограничить срок действия пароля изменение пароля можно запросить при следующем входе пользователя в систему.

Информация, связанная с данной

Системные значения: Обзор паролей

Блокировка изменения пароля (QPWDCHGBLK)

Системное значение Блокировка изменения пароля (QPWDCHGBLK) задает время, в течение которого запрещено изменение пароля после предыдущего изменения.

Изменения, внесенные в это системное значение, вступают в силу немедленно.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в разделе Системные значения защиты.

Таблица 30. Для системного значения QPWDCHGBLK предусмотрены следующие значения:

*NONE	Значение пароля может быть изменено в любой момент.
1 - 99	Пароль можно изменить спустя указанное количество часов после его предыдущего изменения.

Срок действия пароля (QPWDEXPITV)

Системное значение Срок действия пароля (QPWDEXPITV) задает срок действия пароля в днях.

Пользователям, срок действия паролей которых истек, перед входом в систему будет предложено изменить пароль.

Информация о входе в систему

Система:

Срок действия пароля истек. Для входа в систему необходимо изменить пароль.

Предыдущий вход в систему : 10/30/99 14:15:00

Число недопустимых попыток входа в систему . : 3

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 31. Для системного значения QPWDEXPITV предусмотрены следующие значения:

*NOMAX	Срок действия паролей не ограничен.
срок-действия-в-днях	Укажите значение от 1 до 366.

Рекомендуемое значение: от 30 до 90

Примечание: Срок действия паролей можно также указать в отдельных пользовательских профайлах.

Предупреждение об истечении срока действия пароля (QPWDEXPWRN)

Системное значение Предупреждение об истечении срока действия пароля (QPWDEXPWRN) задает число дней, оставшихся до устаревания пароля, когда при входе в систему пользователю показывается предупреждение об истечении срока действия пароля.

Изменения, внесенные в это системное значение, вступают в силу немедленно.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в разделе Системные значения защиты.

Таблица 32. Для системного значения QPWDEXPWRN предусмотрены следующие значения:

7	Если эта опция включена, то предупреждение об истечении срока действия пароля будет показываться за 7 дней до его окончания.
1 - 99	Задаёт число дней, оставшихся до устаревания пароля, когда показывается предупреждение об истечении срока действия пароля.

Рекомендуемое значение: 14 (дней)

Уровень пароля (QPWDLVL)

Уровень пароля позволяет для пользовательских профайлов указывать пароли длиной от 1 до 10 символов, либо длиной от 1 до 128 символов.

В качестве пароля можно указывать пароль-предложение. Термин *пароль-предложение* применяется для обозначения очень длинного пароля, в котором разрешены практически все символы. Между символами пароля-предложения можно применять пробелы, что позволяет указывать в качестве пароля предложения или фрагменты предложений. Единственные ограничения пароля-предложения - это запрет символа звездочки (*) в начале и удаление конечных пробелов. Перед изменением уровня паролей рекомендуется ознакомиться с разделом Планирование изменений уровня пароля.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 33. Для системного значения QPWDLVL предусмотрены следующие значения:

0	<p>Поддерживаются пароли пользовательских профайлов длиной от 1 до 10 символов. Разрешены символы A-Z, 0-9, а также \$, @, # и _ (подчеркивание).</p> <ul style="list-style-type: none">• Это значение следует применять, если система взаимодействует с другими платформами System i, в которых в QPWDLVL указано значение 0 или установлена операционная система до V5R1M0.• Это значение следует применять, если система взаимодействует с другими системами, в которых длина пароля ограничена диапазоном от 1 до 10 символов.• Кроме того, это значение должно применяться, если система обменивается данными с продуктом Поддержка сетевого окружения Windows i5/OS (i5/OS NetServer) или системами, применяющими пароли от 1 до 10 символов. <p>Если в системе значение QPWDLVL равно 0, то операционная система создаст зашифрованный пароль для применения с QPWDLVL 2 и 3. Значение пароля, применяемое для QPWDLVL 2 и 3, совпадает с паролем для QPWDLVL 0 и 1.</p>
---	---

Таблица 33. Для системного значения QPWDLVL предусмотрены следующие значения: (продолжение)

1	<p>Это значение аналогично QPWDLVL 0 со следующим исключением: пароли i5/OS NetServer для клиентов Windows 95/98/ME удаляются из системы.</p> <p>Примечание: Продукт i5/OS Netserver работает с клиентами Windows NT/2000/XP/Vista на уровне паролей с 1 по 3.</p> <p>Если применяется клиент для i5/OS NetServer, то значением QPWDLVL не может быть 1. QPWDLVL 1 улучшает защиту System i, удаляя из системы все пароли i5/OS NetServer.</p>
2	<p>Поддерживаются пароли пользовательских профайлов длиной от 1 до 128 символов. Разрешены символы различного регистра. Пароль может состоять из любых символов с учетом регистра. QPWDLVL 2 рассматривается как уровень совместимости. Этот уровень позволяет вернуться к QPWDLVL 0 или 1, если пароль, созданный на уровне QPWDLVL 2 или 3 удовлетворяет требованиям паролей QPWDLVL 0 или 1.</p> <ul style="list-style-type: none"> • QPWDLVL 2 можно использовать, если система обменивается данными с продуктом Поддержка сетевого окружения Windows i5/OS (i5/OS NetServer) и длина паролей составляет 1-14 символов. • QPWDLVL 2 не следует применять, если система взаимодействует с другими системами System i, в которых в QPWDLVL указано значение 0 или 1, либо установлена операционная система до V5R1M0. • Это значение не следует применять, если система взаимодействует с другими системами, в которых длина пароля ограничена диапазоном от 1 до 10 символов. <p>Изменение значения QPWDLVL на 2 не приводит в удалению из системы зашифрованных паролей.</p>
3	<p>Поддерживаются пароли пользовательских профайлов длиной от 1 до 128 символов. Разрешены символы различного регистра. Пароль может состоять из любых символов с учетом регистра.</p> <ul style="list-style-type: none"> • QPWDLVL 3 не следует применять, если система взаимодействует с другими системами System i, в которых в QPWDLVL указано значение 0 или 1, либо установлена операционная система до V5R1M0. • Это значение не следует применять, если система взаимодействует с другими системами, в которых длина пароля ограничена диапазоном от 1 до 10 символов. • QPWDLVL 3 нельзя использовать, если система обменивается данными с продуктом Поддержка сетевого окружения Windows i5/OS (i5/OS NetServer). <p>Примечание: Продукт i5/OS Netserver работает с клиентами Windows NT/2000/XP/Vista на уровне паролей с 1 по 3. Изменение значения QPWDLVL на 3 приводит к удалению паролей всех пользовательских профайлов, применяемых для QPWDLVL 0 и 1. Для обратного изменения QPWDLVL 3 на QPWDLVL 0 или 1 необходимо предварительно указать QPWDLVL 2. QPWDLVL 2 позволяет создать пароли пользовательских профайлов, совместимые с QPWDLVL 0 и 1, если выполняются требования к длине и синтаксису QPWDLVL 0 и 1.</p>

Переход на уровень пароля, предусматривающий длину пароля от 1 до 128 символов, требует тщательного рассмотрения. Если система взаимодействует с другими системами в сети, все остальные системы также должны поддерживать длинные пароли.

Изменения, внесенные в это системное значение, вступают в силу после IPL. Для просмотра текущих и ожидающих значений уровня пароля воспользуйтесь командой CL Показать атрибуты защиты (DSPSECA).

Минимальная длина пароля (QPWDMINLEN)

Системное значение Минимальная длина пароля (QPWDMINLEN) задает минимальное число символов пароля.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

2. Если системное значение QPWDRULES отличается от *PWDSYSVAL, то это системное значение изменить нельзя, и оно будет игнорироваться при проверке правильности новых паролей.

Таблица 34. Для системного значения QPWDMINLEN предусмотрены следующие значения:

6	Минимальная длина пароля составляет шесть символов.
<i>минимальная-длина</i>	Укажите значение от 1 до 10, если системное значение уровня паролей (QPWDLVL) равно 0 или 1. Укажите значение от 1 до 128, если системное значение уровня паролей (QPWDLVL) равно 2 или 3.

Рекомендуемое значение: 6. Не допускаются пароли, которые можно легко угадать, такие как инициалы или отдельные символы.

Максимальная длина пароля (QPWDMAXLEN)

Системное значение Максимальная длина пароля (QPWDMAXLEN) задает максимальное число символов пароля.

Такое ограничение обеспечивает дополнительную защиту, так как пользователи не могут указать слишком длинные труднозапоминаемые пароли, которые приходится записывать. В некоторых сетях длина пароля не может превышать 8 символов. Данное системное значение позволяет удовлетворить требованиям таких сетей.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.
2. Если системное значение QPWDRULES отличается от *PWDSYSVAL, то это системное значение изменить нельзя, и оно будет игнорироваться при проверке правильности новых паролей.

Таблица 35. Для системного значения QPWDMAXLEN предусмотрены следующие значения:

8	Максимальная длина пароля составляет 8 символов.
<i>максимальная-длина</i>	Укажите значение от 1 до 10, если системное значение уровня паролей (QPWDLVL) равно 0 или 1. Укажите значение от 1 до 128, если системное значение уровня паролей (QPWDLVL) равно 2 или 3.

Рекомендуемое значение: 8

Обязательное изменение пароля (QPWDRQDDIF)

Системное значение Обязательное изменение пароля (QPWDRQDDIF) задает необходимость обязательного изменения паролей.

Такое ограничение обеспечивает дополнительную защиту, так как пользователи не могут указать старые пароли. Кроме того, оно не позволяет снова указать старый пароль, срок действия которого истек.

Примечание: Системное значение QPWDRQDDIF определяет число старых паролей, которые нельзя указывать. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 36. Для системного значения QPWDRQDDIF предусмотрены следующие значения:

<i>Значение</i>	<i>Число старых паролей, которые нельзя указывать</i>
0	Пароли изменять не обязательно.
1	32

Таблица 36. Для системного значения QPWDRQDDIF предусмотрены следующие значения: (продолжение)

Значение	Число старых паролей, которые нельзя указывать
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Рекомендуемое значение: Укажите значение не больше пяти. Системное значение Обязательное изменение пароля (QPWDRQDDIF) совместно с значением Срок действия пароля QPWDEXPITV позволяют запретить применение старых паролей в течение по крайней мере 6 месяцев. Например, если в QPWDEXPITV указать значение 30 (дней), в QPWDRQDDIF - значение 5 (10 уникальных паролей). При этом обычный пользователь, меняющий пароли в соответствии с предупреждениями системы, сможет повторно использовать старый пароль только через 9 месяцев.

Запретить некоторые символы в пароле (QPWDLMTCHR)

Системное значение Запретить некоторые символы в пароле (QPWDLMTCHR) позволяет запретить применение некоторых символов в пароле.

Такое ограничение обеспечивает дополнительную защиту, так как пользователи не могут указать некоторые символы, например, гласные. Запрет гласных не позволяет указывать в качестве паролей реальные слова.

Системное значение QPWDLMTCHR не применяется на уровне пароля (QPWDLVL) 2 и 3. При этом его можно изменить на уровне пароля (QPWDLVL) 2 или 3, но оно вступит в силу только после перехода на уровень 0 или 1.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.
2. Если системное значение QPWDRULES отличается от *PWDSYSVAL, то это системное значение изменить нельзя, и оно будет игнорироваться при проверке правильности новых паролей.

Таблица 37. Для системного значения QPWDLMTCHR предусмотрены следующие значения:

*NONE	В паролях разрешены все символы.
<i>запрещенные-символы</i>	Укажите до 10 запрещенных символов. Допустимы следующие символы : A - Z, 0 - 9, а также специальные символы #, \$, @ и подчеркивание (_).

Рекомендуемое значение: A, E, I, O и U. Кроме того, для совместимости с другими системами рекомендуется запретить специальные символы (#, \$ и @).

Запретить применение последовательности цифр (QPWDLMTAJC)

Системное значение Запретить применение последовательности цифр (QPWDLMTAJC) позволяет запретить цифры, расположенные в соседних позициях в пароле.

Такое ограничение обеспечивает дополнительную защиту, потому что в качестве паролей пользователи не могут указать даты дней рождений, телефонные номера и другие последовательности чисел.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.
2. Если системное значение QPWRULES отличается от *PWDSYSVAL, то это системное значение изменить нельзя, и оно будет игнорироваться при проверке правильности новых паролей.

Таблица 38. Для системного значения QPWDLMTALC предусмотрены следующие значения:

<u>0</u>	Последовательности цифр в паролях разрешены.
1	Последовательности цифр в паролях запрещены.

Запретить применение повторяющихся символов (QPWDLMTREP)

Системное значение Запретить применение повторяющихся символов (QPWDLMTREP) позволяет запретить применение повторяющихся символов в пароле.

Такое ограничение обеспечивает дополнительную защиту, так как пользователи не могут указать пароли, которые можно легко угадать, например, один символ, повторяющийся несколько раз.

Если в системном значении Уровень пароля (QPWDLVL) указано значение 2 или 3, проверка повторяющихся символов выполняется с учетом регистра. Это означает, что символы 'а' и 'А' не совпадают.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.
2. Если системное значение QPWRULES отличается от *PWDSYSVAL, то это системное значение изменить нельзя, и оно будет игнорироваться при проверке правильности новых паролей.

Таблица 39. Для системного значения QPWDLMTREP предусмотрены следующие значения:

<u>0</u>	Совпадающие символы в пароле могут встречаться несколько раз.
1	Каждый символ в пароле может встречаться только один раз.
2	Один символ не может последовательно повторяться в пароле.

В таблице Табл. 40 приведены примеры допустимых паролей в зависимости от системного значения QPWDLMTREP.

Таблица 40. Пароли с повторяющимися символами для QPWDLVL 0 или 1

Пример пароля	QPWDLMTREP 0	QPWDLMTREP 1	QPWDLMTREP 2
A11111	Разрешен	Запрещен	Запрещен
BOBBY	Разрешен	Запрещен	Запрещен
AIRPLANE	Разрешен	Запрещен	Разрешен
N707UK	Разрешен	Запрещен	Разрешен

Таблица 41. Пароли с повторяющимися символами для QPWDLVL 2 и 3

Пример пароля	QPWDLMTREP 0	QPWDLMTREP 1	QPWDLMTREP 2
j222222	Разрешен	Запрещен	Запрещен
ReallyFast	Разрешен	Запрещен	Запрещен
Mom'sApPlePie	Разрешен	Запрещен	Разрешен

Таблица 41. Пароли с повторяющимися символами для QPWDLVL 2 и 3 (продолжение)

Пример пароля	QPWDLMTREP 0	QPWDLMTREP 1	QPWDLMTREP 2
AaBbCcDdEe	Разрешен	Разрешен	Разрешен

Запретить символы в одинаковых позициях (QPWDPOSDIF)

Системное значение Запретить символы в одинаковых позициях (QPWDPOSDIF) позволяет управлять каждой позицией в новом пароле.

Это системное значение обеспечивает дополнительную защиту, потому что пользователи не могут указать в одинаковых позициях нового пароля символы (буквенные и цифровые) из предыдущего пароля.

Если в системном значении Уровень пароля (QPWDLVL) указано значение 2 или 3, проверка символов выполняется с учетом регистра. Это означает, что символы 'а' и 'А' не совпадают.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.
2. Если системное значение QPWDRULES отличается от *PWDSYSVAL, то это системное значение изменить нельзя, и оно будет игнорироваться при проверке правильности новых паролей.

Таблица 42. Для системного значения QPWDPOSDIF предусмотрены следующие значения:

0	Одинаковые символы в одинаковых позициях старого и нового паролей разрешены.
1	Одинаковые символы в одинаковых позициях старого и нового паролей применять запрещено.

Обязательное вхождение в пароль цифр (QPWDRQDDGT)

Системное значение Обязательное вхождение в пароль цифр (QPWDRQDDGT) позволяет указать необходимость обязательного вхождения в пароль цифр. Такое ограничение обеспечивает дополнительную защиту, так как пользователи не смогут указывать пароли, состоящие только из одних букв.

Notes:

1. Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.
2. Если системное значение QPWDRULES отличается от *PWDSYSVAL, то это системное значение изменить нельзя, и оно будет игнорироваться при проверке правильности новых паролей.

Таблица 43. Для системного значения QPWDRQDDGT предусмотрены следующие значения:

0	Цифры в пароле указывать не обязательно.
1	В пароле должна быть хотя бы одна цифра.

Рекомендуемое значение: 1

Правила паролей (QPWDRULES)

Системное значение Правила паролей (QPWDRULES) задает правила, применяемые для проверки правильности паролей. В системном значении QPWDRULES можно указать несколько значений, если не указано значение *PWDSYSVAL.

Изменение этого системного значения вступает в силу при смене пароля.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в разделе Системные значения защиты.

Таблица 44. Для системного значения QPWRULES предусмотрены следующие значения:

*PWDSYSVAL	<p>Это значение указывает, что системное значение QPWRULES игнорируется, и для проверки допустимости пароля применяются другие системные значения. Это значения QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF и QPWDQDDGT.</p> <p>Примечание: Если QPWRULES не равно *PWDSYSVAL, то системные значения QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF и QPWDQDDGT игнорируются при проверке допустимости нового пароля. Кроме того, эти системные значения невозможно изменить, пока QPWRULES не равно *PWDSYSVAL.</p>								
*CHRLMTAJC	<p>Это значение указывает, что пароль не может содержать 2 или более одинаковых смежных символа. Это значение действует аналогично системному значению QPWDLMTREP, равному 2. Это значение нельзя указывать совместно с *CHRLMTREP.</p> <p>Примеры:</p> <table data-bbox="800 961 1230 1077"> <tr> <td>Better.test</td> <td>недопустимый - tt</td> </tr> <tr> <td>fix11bugs</td> <td>недопустимый - 11</td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> </tr> <tr> <td>A1234A1234</td> <td>допустимый</td> </tr> </table>	Better.test	недопустимый - tt	fix11bugs	недопустимый - 11	@12/A78	допустимый	A1234A1234	допустимый
Better.test	недопустимый - tt								
fix11bugs	недопустимый - 11								
@12/A78	допустимый								
A1234A1234	допустимый								
*CHRLMTREP	<p>Это значение указывает, что пароль не может содержать 2 или более одинаковых символа. Это значение действует аналогично системному значению QPWDLMTREP, равному 1. Это значение нельзя указывать совместно с *CHRLMTAJC.</p> <p>Примеры:</p> <table data-bbox="800 1266 1255 1381"> <tr> <td>John.Jones</td> <td>недопустимый - J o n</td> </tr> <tr> <td>THISONEOK</td> <td>недопустимый - 0</td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> </tr> <tr> <td>AaCcEeFfGg</td> <td>допустимый</td> </tr> </table>	John.Jones	недопустимый - J o n	THISONEOK	недопустимый - 0	@12/A78	допустимый	AaCcEeFfGg	допустимый
John.Jones	недопустимый - J o n								
THISONEOK	недопустимый - 0								
@12/A78	допустимый								
AaCcEeFfGg	допустимый								
*DGLMTAJC	<p>Это значение указывает, что пароль не может содержать 2 или более последовательных цифр.</p> <p>Примеры:</p> <table data-bbox="800 1486 1157 1602"> <tr> <td>@12/A78</td> <td>недопустимый</td> </tr> <tr> <td>!@#%a1234.</td> <td>недопустимый</td> </tr> <tr> <td>THISONEOK</td> <td>допустимый</td> </tr> <tr> <td>A1B2C3DE5</td> <td>допустимый</td> </tr> </table>	@12/A78	недопустимый	!@#%a1234.	недопустимый	THISONEOK	допустимый	A1B2C3DE5	допустимый
@12/A78	недопустимый								
!@#%a1234.	недопустимый								
THISONEOK	допустимый								
A1B2C3DE5	допустимый								
*DGLMTFST	<p>Это значение указывает, что первым символом пароля не может быть цифра. Это значение нельзя указывать совместно с *LTRLMTFST и *SPCCHRLMTFST. Если система работает на уровне паролей 0 или 1, то указываются системные функции, например, *DGLMTFST.</p> <p>Примеры:</p> <table data-bbox="800 1812 1206 1925"> <tr> <td>16ST-SW-Roch</td> <td>недопустимый - 1</td> </tr> <tr> <td>99BottlesOfBeer</td> <td>недопустимый - 9</td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> </tr> <tr> <td>Allow-this.1</td> <td>допустимый</td> </tr> </table>	16ST-SW-Roch	недопустимый - 1	99BottlesOfBeer	недопустимый - 9	@12/A78	допустимый	Allow-this.1	допустимый
16ST-SW-Roch	недопустимый - 1								
99BottlesOfBeer	недопустимый - 9								
@12/A78	допустимый								
Allow-this.1	допустимый								

Таблица 44. Для системного значения QPWDRULES предусмотрены следующие значения: (продолжение)

<p>*DGTMLTLST</p>	<p>Это значение указывает, что последним символом пароля не может быть цифра. Это значение нельзя указывать совместно с *LTRLMTLST и *SPCCHRLMTLST.</p> <p>Примеры:</p> <table border="0"> <tr> <td>John.doe12</td> <td>недопустимый - 2</td> </tr> <tr> <td>@12/A78</td> <td>недопустимый - 8</td> </tr> <tr> <td>THISONEOK</td> <td>допустимый</td> </tr> <tr> <td>A1234b123.</td> <td>допустимый</td> </tr> </table>	John.doe12	недопустимый - 2	@12/A78	недопустимый - 8	THISONEOK	допустимый	A1234b123.	допустимый
John.doe12	недопустимый - 2								
@12/A78	недопустимый - 8								
THISONEOK	допустимый								
A1234b123.	допустимый								
<p>*DGTMAXn</p>	<p>Это значение указывает максимальное число цифр в пароле. n - это число от 0 до 9.</p> <p>Можно указывать только одно значение *DGTMAXn. Если задано также значение *DGTMINn, то n для *DGTMAXn должно быть больше или равно n в *DGTMINn.</p> <p>Примеры: для *DGTMAX2</p> <table border="0"> <tr> <td>Q12345678</td> <td>недопустимый - 6 цифр</td> </tr> <tr> <td>3-2-1->Go</td> <td>недопустимый - 1 цифра</td> </tr> <tr> <td>Rick1</td> <td>допустимый</td> </tr> <tr> <td>Ed1-Jeff3</td> <td>допустимый</td> </tr> </table>	Q12345678	недопустимый - 6 цифр	3-2-1->Go	недопустимый - 1 цифра	Rick1	допустимый	Ed1-Jeff3	допустимый
Q12345678	недопустимый - 6 цифр								
3-2-1->Go	недопустимый - 1 цифра								
Rick1	допустимый								
Ed1-Jeff3	допустимый								
<p>*DGTMINn</p>	<p>Это значение указывает минимальное число цифр в пароле. n - это число от 0 до 9.</p> <p>Можно указывать только одно значение *DGTMINn. Если задано также значение *DGTMAXn, то n для *DGTMAXn должно быть больше или равно n в *DGTMINn.</p> <p>Примеры: для *DGTMIN3</p> <table border="0"> <tr> <td>Rick1</td> <td>недопустимый - только 1 цифра</td> </tr> <tr> <td>Ed1-Jeff3</td> <td>недопустимый - только 2 цифры</td> </tr> <tr> <td>3-2-1->Go</td> <td>допустимый</td> </tr> <tr> <td>Q12345678</td> <td>допустимый</td> </tr> </table>	Rick1	недопустимый - только 1 цифра	Ed1-Jeff3	недопустимый - только 2 цифры	3-2-1->Go	допустимый	Q12345678	допустимый
Rick1	недопустимый - только 1 цифра								
Ed1-Jeff3	недопустимый - только 2 цифры								
3-2-1->Go	допустимый								
Q12345678	допустимый								
<p>*LMTSAMPOS</p>	<p>Одинаковые символы в одинаковых позициях старого и нового паролей применять запрещено. Это значение действует аналогично системному значению QPWDPOSDIF.</p> <p>Если пароль password задается командой Изменить пользовательский профайл (CHGUSRPRF) или Создать пользовательский профайл (CRTUSRPRF), то это правило пароля проверить нельзя, так как предыдущий пароль неизвестен.</p> <p>Примеры: для *LMTSAMPOS, где предыдущий пароль - это Vote4Me:</p> <table border="0"> <tr> <td>Victory1</td> <td>недопустимый - V в позиции 1</td> </tr> <tr> <td>Mine2love</td> <td>недопустимый - e в позиции 4</td> </tr> <tr> <td>v0TE-mE</td> <td>допустимый (отличается регистр)</td> </tr> <tr> <td>Allisgood</td> <td>допустимый</td> </tr> </table>	Victory1	недопустимый - V в позиции 1	Mine2love	недопустимый - e в позиции 4	v0TE-mE	допустимый (отличается регистр)	Allisgood	допустимый
Victory1	недопустимый - V в позиции 1								
Mine2love	недопустимый - e в позиции 4								
v0TE-mE	допустимый (отличается регистр)								
Allisgood	допустимый								
<p>*LMTPRFNAME</p>	<p>Пароль в верхнем регистре не должен содержать полный пользовательский профайл.</p> <p>Примеры: для *LMTPRFNAME, где профайл - это JOHNB:</p> <table border="0"> <tr> <td>bigJOHNB9</td> <td>недопустимый - позиции 4-8</td> </tr> <tr> <td>JohnB78</td> <td>недопустимый - позиции 1-5</td> </tr> <tr> <td>J_ohn_B234</td> <td>допустимый</td> </tr> <tr> <td>john_b</td> <td>допустимый</td> </tr> </table>	bigJOHNB9	недопустимый - позиции 4-8	JohnB78	недопустимый - позиции 1-5	J_ohn_B234	допустимый	john_b	допустимый
bigJOHNB9	недопустимый - позиции 4-8								
JohnB78	недопустимый - позиции 1-5								
J_ohn_B234	допустимый								
john_b	допустимый								

Таблица 44. Для системного значения QPWDRULES предусмотрены следующие значения: (продолжение)

*LTRLMTAJC	<p>Это значение указывает, что пароль не может содержать 2 или более последовательных буквы.</p> <p>Примеры:</p> <table border="0"> <tr> <td>John.Smith</td> <td>недопустимый</td> </tr> <tr> <td>THISONEOK</td> <td>недопустимый</td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> </tr> <tr> <td>A1234b1234</td> <td>допустимый</td> </tr> </table>	John.Smith	недопустимый	THISONEOK	недопустимый	@12/A78	допустимый	A1234b1234	допустимый
John.Smith	недопустимый								
THISONEOK	недопустимый								
@12/A78	допустимый								
A1234b1234	допустимый								
*LTRLMTFST	<p>Это значение указывает, что первым символом пароля не может быть буква. Это значение нельзя указывать совместно с *DGTLMTFST и *SPCCHRLMTFST. Если система работает на уровне QPWDLVL 0 или 1, то нельзя указывать совместно *LTRLMTFST и *SPCCHRLMTFST.</p> <p>Примеры:</p> <table border="0"> <tr> <td>John.Smith</td> <td>недопустимый - J</td> </tr> <tr> <td>THISONEOK</td> <td>недопустимый - T</td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> </tr> <tr> <td>16ST-SW-Roch</td> <td>допустимый</td> </tr> </table>	John.Smith	недопустимый - J	THISONEOK	недопустимый - T	@12/A78	допустимый	16ST-SW-Roch	допустимый
John.Smith	недопустимый - J								
THISONEOK	недопустимый - T								
@12/A78	допустимый								
16ST-SW-Roch	допустимый								
*LTRLMTLST	<p>Это значение указывает, что последним символом пароля не может быть буква. Это значение нельзя указывать совместно с *DGTMLTLST и *SPCCHRLMTLST.</p> <p>Примеры:</p> <table border="0"> <tr> <td>John.Smith</td> <td>недопустимый - h</td> </tr> <tr> <td>1Allow.It</td> <td>недопустимый - t</td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> </tr> <tr> <td>(pay*rate)</td> <td>допустимый</td> </tr> </table>	John.Smith	недопустимый - h	1Allow.It	недопустимый - t	@12/A78	допустимый	(pay*rate)	допустимый
John.Smith	недопустимый - h								
1Allow.It	недопустимый - t								
@12/A78	допустимый								
(pay*rate)	допустимый								
*LTRMAXn	<p>Это значение указывает максимальное число букв в пароле. n - это число от 0 до 9.</p> <p>Можно указывать только одно значение *LTRMAXn. Если задано также значение *LTRMINn, то n для *LTRMAXn должно быть больше или равно n в *LTRMINn.</p> <p>Если задано также значение *MIXCASEn, то n для *LTRMAXn должно быть больше или равно удвоенного n в *MIXCASEn.</p> <p>Примеры: для *LTRMAX4</p> <table border="0"> <tr> <td>THISONEOK</td> <td>недопустимый - 5 букв</td> </tr> <tr> <td>John.Smith1</td> <td>недопустимый - 5 букв</td> </tr> <tr> <td>John1423</td> <td>допустимый</td> </tr> <tr> <td>A1b2.#456</td> <td>допустимый</td> </tr> </table>	THISONEOK	недопустимый - 5 букв	John.Smith1	недопустимый - 5 букв	John1423	допустимый	A1b2.#456	допустимый
THISONEOK	недопустимый - 5 букв								
John.Smith1	недопустимый - 5 букв								
John1423	допустимый								
A1b2.#456	допустимый								
*LTRMINn	<p>Это значение указывает минимальное число букв в пароле. n - это число от 0 до 9.</p> <p>Можно указывать только одно значение *LTRMINn. Если задано значение *LTRMAXn, то n для *LTRMAXn должно быть больше или равно n в *LTRMINn.</p> <p>Примеры: для *LTRMIN2</p> <table border="0"> <tr> <td>@12/A78</td> <td>недопустимый - 1 буква</td> </tr> <tr> <td>!@#%a1234</td> <td>недопустимый - 1 буква</td> </tr> <tr> <td>THISONEOK</td> <td>допустимый</td> </tr> <tr> <td>A1234b1234</td> <td>допустимый</td> </tr> </table>	@12/A78	недопустимый - 1 буква	!@#%a1234	недопустимый - 1 буква	THISONEOK	допустимый	A1234b1234	допустимый
@12/A78	недопустимый - 1 буква								
!@#%a1234	недопустимый - 1 буква								
THISONEOK	допустимый								
A1234b1234	допустимый								

Таблица 44. Для системного значения QPWDRULES предусмотрены следующие значения: (продолжение)

<p>*MAXLENnnn</p>	<p>Это значение задает максимальное число символов пароля. nnn - это число от 1 до 128 (без учета нулей в начале). Это значение действует аналогично системному значению QPWDMAXLEN.</p> <p>Если система работает на уровне QPWDLVL 0 или 1, то допустимый диапазон - от 1 до 10. Если система работает на уровне QPWDLVL 2 или 3, то допустимый диапазон - от 1 до 128.</p> <p>Значение nnn должно быть достаточно большим, чтобы учитывать все требования *MIXCASEn, *DGTMAXn, *LTRMAXn, *SPCCHRMAn, первого и последнего символов, и несмежных символов.</p> <p>Если задано также значение *MINLENnnn, то nnn для *MAXLENnnn должно быть больше или равно nnn в *MINLENnnn.</p> <p>Если значение *MAXLENnnn не указано, то предполагается значение *MAXLEN10, если система работает на уровне QPWDLVL 0 или 1, или значение *MAXLEN128, если система работает на уровне QPWDLVL 2 или 3.</p>								
<p>*MINLENnnn</p>	<p>Это значение задает минимальное число символов пароля. nnn - это число от 1 до 128 (без учета нулей в начале).</p> <p>Если система работает на уровне QPWDLVL 0 или 1, то допустимый диапазон - от 1 до 10. Если система работает на уровне QPWDLVL 2 или 3, то допустимый диапазон - от 1 до 128.</p> <p>Если задано также значение *MAXLENnnn, то nnn для *MAXLENnnn должно быть больше или равно nnn в *MINLENnnn.</p> <p>Если не указано значение *MINLENnnn, то предполагается значение *MINLEN1.</p>								
<p>*MIXCASEn</p>	<p>Указывает, что пароль должен содержать не менее n символов в верхнем и n символов в нижнем регистре. n - это число от 0 до 9. Это значение недопустимо, если система работает на уровне QPWDLVL 0 или 1, потому что пароли должны указываться в верхнем регистре.</p> <p>Можно указывать только одно значение *MIXCASEn.</p> <p>Если задано значение *LTRMAXn, то n для *LTRMAXn должно быть больше или равно удвоенного n в *MIXCASEn.</p> <p>Примеры: для *MIXCASE2</p> <table border="0"> <tr> <td>@12/A78bC</td> <td>недопустимый - отсутствует 1 символ в нижнем регистре</td> </tr> <tr> <td>THISONEOK</td> <td>недопустимый - отсутствуют 2 символа в нижнем регистре</td> </tr> <tr> <td>ThisIsOkay</td> <td>допустимый</td> </tr> <tr> <td>Allow-It</td> <td>допустимый</td> </tr> </table>	@12/A78bC	недопустимый - отсутствует 1 символ в нижнем регистре	THISONEOK	недопустимый - отсутствуют 2 символа в нижнем регистре	ThisIsOkay	допустимый	Allow-It	допустимый
@12/A78bC	недопустимый - отсутствует 1 символ в нижнем регистре								
THISONEOK	недопустимый - отсутствуют 2 символа в нижнем регистре								
ThisIsOkay	допустимый								
Allow-It	допустимый								

Таблица 44. Для системного значения QPWDRULES предусмотрены следующие значения: (продолжение)

<p>*REQANY3</p>	<p>Указывает, что пароль должен содержать не менее трех из следующих четырех типов символов.</p> <ul style="list-style-type: none"> • Прописные буквы • Строчные буквы • Цифры • Специальные символы <p>Если система работает на уровне QPWDLVL 0 или 1, то *REQANY3 аналогично тому, как если бы были указаны одновременно *DGTMIN1, *LTRMIN1 и *SPCCHRMIN1.</p> <p>Примеры:</p> <table style="width: 100%; border: none;"> <tr> <td>THISONEOK</td> <td>недопустимый</td> <td>- только 1 тип</td> </tr> <tr> <td>@12/-78</td> <td>недопустимый</td> <td>- только 2 типа</td> </tr> <tr> <td>A1234b1234</td> <td>допустимый</td> <td></td> </tr> <tr> <td>John.Smith</td> <td>допустимый</td> <td></td> </tr> <tr> <td>peter(21)</td> <td>допустимый</td> <td></td> </tr> </table>	THISONEOK	недопустимый	- только 1 тип	@12/-78	недопустимый	- только 2 типа	A1234b1234	допустимый		John.Smith	допустимый		peter(21)	допустимый	
THISONEOK	недопустимый	- только 1 тип														
@12/-78	недопустимый	- только 2 типа														
A1234b1234	допустимый															
John.Smith	допустимый															
peter(21)	допустимый															
<p>*SPCCHRLMTAJC</p>	<p>Это значение указывает, что пароль не может содержать 2 или более последовательных специальных символа. Специальный символ - это символ, значение unicode которого не может быть представлено в виде буквы или цифры.</p> <p>Примеры:</p> <table style="width: 100%; border: none;"> <tr> <td>Big//Box</td> <td>недопустимый</td> </tr> <tr> <td>this->way</td> <td>недопустимый</td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> </tr> <tr> <td>John.Smith</td> <td>допустимый</td> </tr> </table>	Big//Box	недопустимый	this->way	недопустимый	@12/A78	допустимый	John.Smith	допустимый							
Big//Box	недопустимый															
this->way	недопустимый															
@12/A78	допустимый															
John.Smith	допустимый															
<p>*SPCCHRLMTFST</p>	<p>Это значение указывает, что первым символом пароля не может быть специальный символ. Специальный символ - это символ, значение unicode которого не может быть представлено в виде буквы или цифры.</p> <p>Это значение нельзя указывать совместно с *DGTLMFST и *LTRLMFST. Если система работает на уровне QPWDLVL 0 или 1, то нельзя указывать совместно *LTRLMFST и *SPCCHRLMTFST.</p> <p>Примеры:</p> <table style="width: 100%; border: none;"> <tr> <td>(2+2equals4)</td> <td>недопустимый</td> <td>- (</td> </tr> <tr> <td>#fred/#charlie</td> <td>недопустимый</td> <td>- #</td> </tr> <tr> <td>1Good->one12</td> <td>допустимый</td> <td></td> </tr> <tr> <td>A1234b1234</td> <td>допустимый</td> <td></td> </tr> </table>	(2+2equals4)	недопустимый	- (#fred/#charlie	недопустимый	- #	1Good->one12	допустимый		A1234b1234	допустимый				
(2+2equals4)	недопустимый	- (
#fred/#charlie	недопустимый	- #														
1Good->one12	допустимый															
A1234b1234	допустимый															
<p>*SPCCHRLMTLST</p>	<p>Это значение указывает, что последним символом пароля не может быть специальный символ. Специальный символ - это символ, значение unicode которого не может быть представлено в виде буквы или цифры.</p> <p>Это значение нельзя указывать совместно с *DGTMLTST и *LTRMLTST.</p> <p>Примеры:</p> <table style="width: 100%; border: none;"> <tr> <td>A1234b123.</td> <td>недопустимый</td> <td>- .</td> </tr> <tr> <td>>John.Doe<</td> <td>недопустимый</td> <td>- <</td> </tr> <tr> <td>THISONEOK</td> <td>допустимый</td> <td></td> </tr> <tr> <td>@12/A78</td> <td>допустимый</td> <td></td> </tr> </table>	A1234b123.	недопустимый	- .	>John.Doe<	недопустимый	- <	THISONEOK	допустимый		@12/A78	допустимый				
A1234b123.	недопустимый	- .														
>John.Doe<	недопустимый	- <														
THISONEOK	допустимый															
@12/A78	допустимый															

Таблица 44. Для системного значения QPWDRULES предусмотрены следующие значения: (продолжение)

<p>*SPCCHRMAXn</p>	<p>Это значение указывает максимальное число специальных символов в пароле. n - это число от 0 до 9. Специальный символ - это символ, значение unicode которого не может быть представлено в виде буквы или цифры.</p> <p>Можно указывать только одно значение *SPCCHRMAXn. Если задано значение *SPCCHRMINn, то n для *SPCCHRMAXn должно быть больше или равно n в *SPCCHRMINn.</p> <p>Примеры: для *SPCCHRMAX3</p> <p>@12/A78.b# недопустимый - 1 !@#\$\$%a1234 недопустимый - 2 TH1\$ONEOK допустимый A1234b-234 допустимый</p>
<p>*SPCCHRMINn</p>	<p>Это значение указывает минимальное число специальных символов в пароле. n - это число от 0 до 9. Специальный символ - это символ, значение unicode которого не может быть представлено в виде буквы или цифры.</p> <p>Можно указывать только одно значение *SPCCHRMINn. Если задано значение *SPCCHRMAXn, то n для *SPCCHRMAXn должно быть больше или равно n в *SPCCHRMINn.</p> <p>Примеры: для *SPCCHRMIN4</p> <p>Su@us.ibm.com недопустимый - 1 123+45=168 недопустимый - 2 A.B@us.ibm.com допустимый (24/8=3) допустимый</p>

Программа подтверждения паролей (QPWDVLDPGM)

Программа подтверждения паролей (QPWDVLDPGM) позволяет управлять проверкой новых паролей.

Если в системном значении QPWDVLDPGM указано значение *REGFAC или имя программы, то система выполняет одну или несколько программ после подтверждения нового пароля в соответствии с параметрами системы управления паролями. С помощью этих программ можно выполнить дополнительную проверку пользовательских паролей перед их подтверждением в системе.

Программа подтверждения паролей должна быть расположена в системном пуле дисков (ASP) или основном пользовательском ASP.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 45. Для системного значения QPWDVLDPGM предусмотрены следующие значения:

<p>*NONE</p>	<p>Пользовательская программа не применяется. Это относится к программам подтверждения паролей, зарегистрированным в средстве регистрации программ выхода.</p>
<p>*REGFAC</p>	<p>Программа подтверждения паролей загружается из средства регистрации, точка выхода QIBM_QSY_VLD_PASSWRD. В средстве регистрации может быть указано несколько программ подтверждения паролей. Программы вызываются последовательно до тех пор, пока одна из них не укажет на неправильность пароля или все не подтвердят допустимость пароля.</p>

Таблица 45. Для системного значения QPWDVLDPGM предусмотрены следующие значения: (продолжение)

<i>программа</i>	Укажите имя пользовательской программы подтверждения паролей длиной от 1 до 10 символов. Если текущее или ожидающее значение системного значения Уровень пароля (QPWDLVL) равно 2 или 3, то имя программы указать нельзя.
<i>библиотека</i>	Укажите имя библиотеки, в которой расположена пользовательская программа. Если имя библиотеки не указано, то поиск программы выполняется с помощью списка библиотек (*LIBL) пользователя, изменяющего это системное значение. Рекомендуется использовать библиотеку QSYS.

Работа с программой подтверждения паролей

Если в системном значении QPWDVLDPGM указано значение *REGFAC или имя программы, то с помощью команды Изменить пароль (CHGPWD) или API Изменить пароль (QSYCHGPW) вызывается одна или несколько программ. Программы вызываются только в том случае, если новый пароль прошел все тесты, указанные в системных значениях управления паролями.

Если систему необходимо восстановить после сбоя, поместите программу подтверждения паролей в библиотеку QSYS. Такой подход позволяет загружать программу подтверждения паролей после восстановления библиотеки QSYS.

Если в системном значении QPWDVLDPGM указано имя программы, то система передает программе подтверждения паролей следующие параметры:

Таблица 46. Параметры, передаваемые программе подтверждения паролей

Должность	Тип	Длина	Описание
1	*CHAR	10	Новый пароль, указанный пользователем.
2	*CHAR	10	Старый пароль.
3	*CHAR	1	Код возврата: ноль - для допустимого пароля, отличный от нуля - для неправильного пароля.
4 ¹	*CHAR	10	Имя пользователя.
1	Положение 4 необязательное.		

Если в системном значении QPWDVLDPGM указано значение *REGFAC, за дополнительной информацией о параметрах, передаваемых программе подтверждения паролей, обратитесь к информации о Программе выхода защиты, приведенной в руководстве по системному API.

Если программа определяет, что новый пароль недопустим, вы можете отправить собственное сообщение об исключении (с помощью команды SNDPGMMSG) или указать код возврата отличный от нуля, в соответствии с которым выводится сообщение об ошибке. Сообщения об исключении для пользовательской программы должны создаваться с помощью опции DMPLST(*NONE) команды Добавить описание сообщения (ADDMSGD).

Новый пароль принимается только в том случае, если пользовательская программа завершается без аварийных сообщений с кодом возврата, равным 0. Так как изначально код возврата указан для недопустимых паролей (не равен нулю), то для изменения пароля программа подтверждения паролей должна указать нулевой код возврата.

Внимание: Текущий и новый пароли передаются программе проверки в незашифрованном виде. Программа проверки может хранить пароли в базе данных, что может привести к утечке конфиденциальной информации. Убедитесь, что функции программы проверки паролей проверены системным администратором и все изменения, вносимые в эту программу, находятся под жестким контролем.

Ниже приведен пример программы подтверждения паролей на языке CL, вызываемой, если ее имя указано в системном значении QPWDVLDPGM. Этот пример позволяет проверить, что пароль не изменялся несколько раз в день. Для дополнительной проверки паролей вы можете добавить необходимые команды:

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе Глава 10, “Лицензия на исходный код и отказ от обязательств”, на стр. 325.

```

/*****/
/* Имя: PWDVALID - Проверка паролей */
/* */
/* Предназначение: Позволяет изменять пароль */
/* не более одного раза в день, */
/* если срок его действия не истек */
/*****/
PGM (&NEW &OLD &RTNCD &USER)
DCL VAR(&NEW) TYPE(*CHAR) LEN(10)
DCL VAR(&OLD) TYPE(*CHAR) LEN(10)
DCL VAR(&RTNCD) TYPE(*CHAR) LEN(1)
DCL VAR(&USER) TYPE(*CHAR) LEN(10)
DCL VAR(&JOBDATE) TYPE(*CHAR) LEN(6)
DCL VAR(&PWDCHGDAT) TYPE(*CHAR) LEN(6)
DCL VAR(&PWDEXP) TYPE(*CHAR) LEN(4)
/* Получение текущей даты и преобразование ее в формат ГМД */
RTVJOBA DATE(&JOBDATE)
CVTDAT DATE(&JOBDATE) TOVAR(&JOBDATE) +
TOFMT(*YMD) TOSEP(*NONE)
/* Получение даты последнего изменения пароля и */
/* проверка его срока действия */
RTVUSRPRF USRPRF(&USER) PWDCHGDAT(&PWDCHGDAT)+
PWDEXP(&PWDEXP)
/* Сравнение двух дат */
/* Если они равны и срок действия пароля не */
/* истек, то отправить сообщение *ESCAPE во */
/* избежание изменений, иначе установить код */
/* возврата, разрешающий изменения */
IF (&JOBDATE=&PWDCHGDAT *AND &PWDEXP='*NO ') +
SNDPGMMSG MSGID(CPF9898) MSGF(QCPFMSG) +
MSGDTA('Пароль можно изменять только +
раз в день') +
MSGTYPE(*ESCAPE)
ELSE CHGVAR &RTNCD '0'
ENDPGM

```

Ниже приведен пример программы подтверждения паролей на языке CL, вызываемой, если в системном значении QPWDVLDLVL указано значение *REGFAC.

Этот пример позволяет убедиться, что пароль указан в кодировке CCSID 37 (если он указан в CCSID 13488, то пароль преобразуется в CCSID 37), пароль не заканчивается на цифру, а также в нем не содержится имя пользовательского профайла. В примере предполагается, что создан файл сообщений (PWDERRORS) и в него добавлены описания сообщений (PWD0001 и PWD0002). Для дополнительной проверки паролей вы можете добавить необходимые команды:

```

/*****/
/* */
/* Имя: PWDEXITPGM1 - Программа выхода проверки паролей 1 */
/* */
/* Проверяет пароли в случае QPWDVLDPGM(*REGFAC). */
/* Программа регистрируется с помощью команды CL */
/* ADDEXITPGM для точки выхода QIBM_QSY_VLD_PASSWRD. */
/* */
/* */
/* ПРЕДПОЛОЖЕНИЯ: если была использована команда CHGPWD, */
/* то паролем CCSID будет пароль задания по умолчанию */
/* (CCSID 37). Если был использован API QSYCHGPW, то */

```

```

/* CCSID пароля будет равен UNICODE CCSID 13488. */
/*****/

PGM PARM(&EXINPUT &RTN)
DCL &EXINPUT *CHAR 1000
DCL &RTN *CHAR 1

DCL &UNAME *CHAR 10
DCL &NEWPW *CHAR 256
DCL &NPOFF *DEC 5 0
DCL &NPLEN *DEC 5 0
DCL &INDX *DEC 5 0
DCL &INDX2 *DEC 5 0
DCL &INDX3 *DEC 5 0
DCL &UNLEN *DEC 5 0

DCL &XLTCHR2 *CHAR 2 VALUE(X'0000')
DCL &XLTCHR *DEC 5 0
DCL &XLATEU *CHAR 255 VALUE('..... +
!"#$( )*+,-./0123456789:;<=>?+
@ABCDEFGHIJKLMNPQRSTUVWXYZ[\]^_+
`ABCDEFGHIJKLMNPQRSTUVWXYZ{|}~.+
.....+
.....+
.....+
.....')

DCL &XLATEC *CHAR 255 VALUE('..... +
.....+
.....+
.....+
.ABCDEFGHI.....JKLMNPQR.....+
..STUVWXYZ.....+
.....+
.....')

/*****/
/* Формат ввода: */

/* Положение Описание */
/* 001 - 020 Имя точки выхода */
/* 021 - 028 Имя формата точки выхода */
/* 029 - 032 Уровень пароля (двоичный) */
/* 033 - 042 Имя пользовательского профайла */
/* 043 - 044 Зарезервировано */
/* 045 - 048 Смещение относительно старого пароля (двоичное) */
/* 049 - 052 Длина старого пароля (двоичная) */
/* 053 - 056 CCSID старого пароля (двоичный) */
/* 057 - 060 Смещение относительно нового пароля (двоичное) */
/* 061 - 064 Длина нового пароля (двоичная) */
/* 065 - 068 CCSID нового пароля (двоичный) */
/* ??? - ??? прежний пароль */
/* ??? - ??? новый пароль */
/* */
/*****/

/*****/
/* Создание общего монитора для программы. */
/*****/

MONMSG CPF0000
/* Предполагается, что новый пароль допустим */
CHGVAR &RTN VALUE('0') /* принять */
/* Получение имени пользователя, длины, смещения и значения нового пароля. */
CHGVAR &NPLEN VALUE(EXINPUT 61 4)
CHGVAR &NPOFF VALUE(EXINPUT 57 4) + 1

```



```

CHGVAR &UNAME VALUE(EXINPUT 33 10))
CHGVAR &NEWPW VALUE(EXINPUT &NPOFF &NPLEN))
/* Если CCSID равен 13488, то, вероятно, применялся API QSYCHGPW, */
/* преобразующий пароли в UNICODE CCSID 13488. Поэтому преобразуется */
/* в CCSID 37, если это возможно, иначе выдается ошибка */
IF COND(EXINPUT 65 4) = 13488) THEN(DO)
  CHGVAR &INDX2 VALUE(1)
  CHGVAR &INDX3 VALUE(1)
  CVT1:
  CHGVAR &XLTCHR VALUE(NEWPW &INDX2 2))
  IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
    CHGVAR &RTN VALUE('3') /* reject */
    SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
    GOTO DONE
  ENDDO
  CHGVAR NEWPW &INDX3 1) VALUE(XLATEU &XLTCHR 1))
  CHGVAR &INDX2 VALUE(&INDX2 + 2)
  CHGVAR &INDX3 VALUE(&INDX3 + 1)
  IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT1)
  GOTO CVT1
  ECVT1:
  CHGVAR &NPLEN VALUE(&INDX3 - 1)
  CHGVAR EXINPUT 65 4) VALUE(X'00000025')
ENDDO

/* Проверка CCSID нового пароля - должно быть указано значение 37 */
IF COND(EXINPUT 65 4) *NE 37) THEN(DO)
  CHGVAR &RTN VALUE('3') /* reject */
  SNDPGMMSG MSG('CCSID нового пароля должен быть равен 37')
  GOTO DONE
ENDDO

/* Изменение всех символов пароля на прописные буквы */
CHGVAR &INDX2 VALUE(1)
CHGVAR &INDX3 VALUE(1)
CVT4:
  CHGVAR XLTCHR2 2 1) VALUE(NEWPW &INDX2 1))
  CHGVAR &XLTCHR VALUE(XLTCHR2 1 2))
  IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
    CHGVAR &RTN VALUE('3') /* reject */
    SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
    GOTO DONE
  ENDDO
  IF COND(XLATEC &XLTCHR 1) *NE '.' ) +
  THEN(CHGVAR NEWPW &INDX3 1) VALUE(XLATEC &XLTCHR 1)))
  CHGVAR &INDX2 VALUE(&INDX2 + 1)
  CHGVAR &INDX3 VALUE(&INDX3 + 1)
  IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT4)
  GOTO CVT4
  ECVT4:

/* Проверка, не указана ли цифра в последней позиции нового пароля */
IF COND(NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '9') THEN(GOTO ERROR1)

/* Проверка, не содержится ли в новом пароле имя пользовательского профайла */
CHGVAR &UNLEN VALUE(1)
LOOP2: /* FIND LENGTH OF USER NAME */
  IF COND(UNAME &UNLEN 1) *NE ' ') THEN(DO)

```

```

CHGVAR &UNLEN VALUE(&UNLEN + 1)
IF COND(&UNLEN = 11) THEN(GOTO ELOOP2)
GOTO LOOP2
ENDDO
ELOOP2:
CHGVAR &UNLEN VALUE(&UNLEN - 1)

/* Проверка, не содержится ли в новом пароле имя пользователя */
IF COND(&UNLEN *GT &NPLEN) THEN(GOTO ELOOP3)
CHGVAR &INDX VALUE(1)
LOOP3:
IF COND(NEWPW &INDX &UNLEN) = UNAME 1 &UNLEN)) +
THEN(GOTO ERROR2)
IF COND((&INDX + &UNLEN + 1) *LT 128) THEN(DO)
CHGVAR &INDX VALUE(&INDX + 1)
GOTO LOOP3
ENDDO
ELOOP3:

/* Новый пароль указан правильно */
GOTO DONE

Ошибка 1: /* Новый пароль заканчивается на цифру */
CHGVAR &RTN VALUE('3') /* reject */
SNDPGMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0001) MSGF(QSYS/PWDERRORS)
GOTO DONE

Ошибка 2: /* В новом пароле содержится имя пользователя */
CHGVAR &RTN VALUE('3') /* reject */
SNDPGMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0002) MSGF(QSYS/PWDERRORS)
GOTO DONE

DONE:
ENDPGM

```

Системные значения, связанные с контролем

Контроль операций в системе является важной составной частью защиты системы. Он позволяет обнаруживать недопустимые действия в системе и вторжения. Для контроля в операционной системе применяются специальные системные значения i5/OS.

Описание:

Задача:

Системные значения, позволяющие управлять контролем за действиями в системе.

Средства для ее решения:

WRKSYSVAL *SEC (команда Работа с системными значениями)

Права доступа:

*AUDIT

Запись в журнале:

SV

Прим.: Изменения вступают в силу немедленно. IPL не требуется.

Следующие системные значения управляют контролем за действиями в системе:

QAUDCTL

Контроль за действиями

QAUDENDACN

Действие при сбое контроля

QAUDFRCLVL

Число записей в журнале контроля перед их сохранением

QAUDLVL

Уровень контроля

QAUDLVL2

Расширение уровня контроля

QCRTOBJAUD

Создать контроль по умолчанию

Управление контролем (QAUDCTL)

Системное значение Управление контролем (QAUDCTL) позволяет осуществлять контроль за действиями.

Это системное значение выполняет роль переключателя для следующих системных значений и операций:

- Системных значений QAUDLVL и QAUDLVL2
- Контроля за действиями, определенного для объектов с помощью команд Изменить контроль за объектами (CHGOBJAUD), Изменить значение контроля (CHGAUD) и Изменить контроль DLO (CHGDLOAUD)
- Контроль, определенный для пользователей с помощью команды Изменить пользовательский контроль (CHGUSRAUD)

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

В системном значении QAUDCTL можно указать несколько значений, если в нем не указано значение *NONE.

Таблица 47. Для системного значения QAUDCTL предусмотрены следующие значения:

*NONE	Контроль за пользовательскими действиями и объектами не ведется.
*NOTAVL	Означает, что системное значение недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение системному значению нельзя.
*OBJAUD	Выполняется контроль за объектами, выбранными с помощью команд CHGOBJAUD, CHGDLOAUD или CHGAUD.
*AUDLVL	Выполняется контроль за функциями, указанными в системных значениях QAUDLVL и QAUDLVL2 и в параметре AUDLVL отдельных пользовательских профайлов. Уровень контроля для пользователя указывается с помощью команды Изменить пользовательский контроль (CHGUSRAUD).
*NOQTEMP	Если объект расположен в библиотеке QTEMP, то большинство действий не контролируется. Дополнительная информация приведена в разделе Глава 9, “Контроль эффективности защиты системы System i”, на стр. 271. Это значение следует указывать совместно с *OBJAUD или *AUDLVL.
	За полным описанием процесса управления контролем для вашей системы обратитесь к разделу “Планирование контроля за действиями” на стр. 278.

Действие при сбое контроля (QAUDENDACN)

Системное значение Действие при сбое контроля (QAUDENDACN) определяет действие, выполняемое системой, если контроль активен и не удается записать данные в журнал контроля.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений

приведены в главе Системные значения защиты.

Таблица 48. Для системного значения QAUDENDACN предусмотрены следующие значения:

*NOTAVL	Означает, что системное значение недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение системному значению нельзя.
*NOTIFY	В очередь сообщений QSYSOPR и QSYSMSG (если она существует) с интервалом в один час отправляются сообщения CPI2283, до тех пор, пока не будет успешно перезапущена функция контроля. В системном значении QAUDCTL указывается значение *NONE, запрещающее занесение дополнительных записей в журнал контроля. Обработка продолжается. Если IPL выполняется до перезапуска контроля, во время IPL в очереди сообщений QSYSOPR и QSYSMSG отправляется сообщение CPI2284.
*PWRDWN SYS	Если не удалось занести запись в журнал контроля, то система немедленно выключается. Системный блок выдает системный информационный код (SRC) B900 3D10. При последующем включении система переводится в состояние с ограничениями. Это означает, что управляющая подсистема находится в состоянии с ограничениями, другие подсистемы не работают и вход в систему разрешен только с консоли. В системном значении QAUDCTL указано значение *NONE. Для выполнения IPL пользователь, работающий с консолью, должен обладать специальными правами доступа *ALLOBJ и *AUDIT.

Рекомендуемое значение: В большинстве случаев рекомендуется значение *NOTIFY. Если стратегия защиты предусматривает контроль за всеми действиями, укажите значение *PWRDWN SYS.

Система не может заносить записи в журнал контроля только в очень необычных условиях. Однако, если это действительно произошло и в системном значении указано *PWRDWN SYS, то система завершит работу в аварийном режиме. Это может привести в длительной загрузке начальной программы (IPL) при следующем включении системы.

Число записей в журнале контроля перед их сохранением (QAUDFRCLVL)

Системное значение Уровень выгрузки записей контроля (QAUDFRCLVL) определяет частоту сохранения новых записей журнала контроля из оперативной памяти во вспомогательную память. Это системное значение определяет объем данных, которые могут быть потеряны в случае аварийного завершения работы системы.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 49. Для системного значения QAUDFRCLVL предусмотрены следующие значения:

*NOTAVL	Означает, что системное значение недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение системному значению нельзя.
*SYS	Время сохранения записей из журнала контроля определяется в соответствии с внутренней производительностью системы.
<i>число-записей</i>	Укажите число записей от 1 до 100, при достижении которого записи сохраняются из оперативной памяти во вспомогательную. Чем меньше число, тем сильнее снижение производительности.

Рекомендуемое значение: *SYS. Оно позволяет получить наилучшую производительность. Если требуется, чтобы в случае аварийного завершения работы системы сохранялись все записи, укажите 1 (это может снизить производительность).

Уровень контроля (QAUDLVL)

Системное значение Уровень контроля (QAUDLVL) совместно с системным значением QAUDLVL2 определяет события, связанные с защитой, которые заносятся в журнал контроля за действиями (QAUDJRN) всех пользователей.

В системном значении QAUDLVL можно указать несколько значений, если в нем не указано значение *NONE.

Для того чтобы системное значение QAUDLVL вступило в силу, в системном значении должно быть указано значение *AUDLVL.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 50. Для системного значения QAUDLVL предусмотрены следующие значения:

*NONE	События, управляемые с помощью системных значений QAUDLVL и QAUDLVL2, в журнал не заносятся. События регистрируются в соответствии с значениями AUDLVL пользовательских профайлов отдельных пользователей.
*NOTAVL	Означает, что системное значение недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение системному значению нельзя.
*AUDLVL2	Для определения контролируемых действий, связанных с защитой, применяется как системное значение QAUDLVL, так и QAUDLVL2.
*ATNEVT	Регистрируются события, связанные с нажатием клавиши Attention.
*AUTFAIL	Регистрируются события, связанные с ошибками прав доступа.
*CREATE	Регистрируются операции, связанные с созданием объектов.
*DELETE	Регистрируются операции, связанные с удалением объектов.
*JOBBAS	Контролируются основные функции заданий.
*JOBCHGUSR	Контролируются изменения профайла пользователя или группы активной нити.
*JOBDTA	Регистрируются действия, связанные с изменением объектов. *JOBDTA включает значения *JOBBAS и *JOBCHGUSR, позволяющие точнее настроить контроль. Если указаны оба эти значения, то результат будет аналогичен тому, как если бы было указано только значение *JOBDTA.
*NETBAS	Контролируются основные сетевые функции.
*NETCLU	Контролируются операции, связанные с кластером и группой ресурсов кластера.
*NETCMN	Контролируются сетевые функции и функции связи. Значение *NETCMN состоит из нескольких значений контроля, позволяющих более точно настроить функцию контроля. Они перечислены ниже: *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	Контролируются сбои сети.
*NETSCK	Контролируются задачи сокетов.

Таблица 50. Для системного значения QAUDLVL предусмотрены следующие значения: (продолжение)

*OBJMGT	Регистрируются операции по перемещению и переименованию объектов.
*OFCSRV	Регистрируются изменения, вносимые в системный каталог рассылки и действия, связанные с электронной почтой.
*OPTICAL	Регистрируется работа с оптическими томами.
*PGMADP	Регистрируются случаи получения прав доступа от программы, принимающей права доступа.
*PGMFAIL	Регистрируются нарушения целостности системы.
*PRTDTA	Регистрируются такие действия, как печать буферного файла, отправка вывода непосредственно на печать, отправка вывода на удаленный принтер.
*SAVRST	Регистрируются операции по сохранению и восстановлению объектов.
*SECCFG	Контролируется конфигурация защиты.
*SECDIRSRV	Контролируются изменения и обновления при выполнении функций службы каталогов.
*SECIPC	Контролируются изменения, вносимые в обмен данными между процессами.
*SECNAS	Контролируются действия службы сетевой идентификации.
*SECRUN	Контролируются базовые функции защиты.
*SECCKD	Контролируются дескрипторы сокетов.
*SECURITY	Регистрируются функции, связанные с защитой. *SECURITY состоит из нескольких значений, позволяющих выполнить более точную настройку контроля. Эти значения перечислены ниже: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECCKD *SECVFY *SECVLDL
*SECVFY	Контролируется работа с функциями проверки.
*SECVLDL	Контролируются изменения, вносимые в объекты контрольных списков.
*SERVICE	Контролируется работа со служебными средствами.
*SPLFDA	Регистрируются действия, выполняемые над буферными файлами.
*SYSMGT	Регистрируется работа с функциями управления системами.

Ссылки, связанные с данной

“Планирование контроля действий” на стр. 278

Для контроля действий используются системные значения QAUDCTL (управление контролем), QAUDLVL (уровень контроля), QAUDLVL2 (расширение уровня контроля), а также параметр AUDLVL (контроль действий) из пользовательских профайлов.

Расширение уровня контроля (QAUDLVL2)

Системное значение Расширение уровня контроля (QAUDLVL2) необходимо для применения более шестнадцати значений контроля.

Если в системном значении QAUDLVL указано значение *AUDLVL2, то значения контроля также проверяются в системном значении QAUDLVL2. В системном значении QAUDLVL2 можно указать

несколько значений, если в нем не указано значение *NONE. Для того чтобы системное значение QAUDLVL2 вступило в силу, в системном значении QAUDCTL должно быть указано значение *AUDLVL, а в системном значении QAUDLVL- значение *AUDLVL2.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 51. Для системного значения QAUDLVL2 предусмотрены следующие значения:

*NONE	В этом системном значении не содержатся значения контроля.
*NOTAVL	Означает, что системное значение недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение системному значению нельзя.
*ATNEVT	Регистрируются события, связанные с нажатием клавиши Attention.
*AUTFAIL	Регистрируются события, связанные с ошибками прав доступа.
*CREATE	Регистрируются операции, связанные с созданием объектов.
*DELETE	Регистрируются операции, связанные с удалением объектов.
*JOBBAS	Контролируются основные функции заданий.
*JOBCHGUSR	Контролируются изменения профайла пользователя или группы активной нити.
*JOBDTA	Регистрируются действия, связанные с изменением объектов. *JOBDTA включает значения *JOBBAS и *JOBCHGUSR, позволяющие точнее настроить контроль. Если указаны оба эти значения, то результат будет аналогичен тому, как если бы было указано только значение *JOBDTA.
*NETBAS	Контролируются основные сетевые функции.
*NETCLU	Контролируются операции, связанные с кластером и группой ресурсов кластера.
*NETCMN	Контролируются сетевые функции и функции связи. Значение *NETCMN состоит из нескольких значений контроля, позволяющих более точно настроить функцию контроля. Они перечислены ниже: *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	Контролируются сбои сети.
*NETSCK	Контролируются задачи сокетов.
*OBJMGT	Регистрируются операции по перемещению и переименованию объектов.
*OFCSRVR	Регистрируются изменения, вносимые в системный каталог рассылки и действия, связанные с электронной почтой.
*OPTICAL	Регистрируется работа с оптическими томами.
*PGMADP	Регистрируются случаи получения прав доступа от программы, принимающей права доступа.
*PGMFAIL	Регистрируются нарушения целостности системы.
*PRTDTA	Регистрируются такие действия, как печать буферного файла, отправка вывода непосредственно на печать, отправка вывода на удаленный принтер.
*SAVRST	Регистрируются операции по восстановлению.
*SEC CFG	Контролируется конфигурация защиты.
*SEC DIRSRV	Контролируются изменения и обновления при выполнении функций службы каталогов.

Таблица 51. Для системного значения QAUDLVL2 предусмотрены следующие значения: (продолжение)

*SECIPC	Контролируются изменения, вносимые в обмен данными между процессами.
*SECNAS	Контролируются действия службы сетевой идентификации.
*SECRUN	Контролируются базовые функции защиты.
*SECCKD	Контролируются дескрипторы сокетов.
*SECURITY	Регистрируются функции, связанные с защитой. Значение *SECURITY состоит из нескольких значений контроля, позволяющих более точно настроить функцию контроля. Эти значения перечислены ниже: *SECCFG *SEC_DIRSRV *SECIPC *SECNAS *SECRUN *SECCKD *SECVFY *SECVLDL
*SECVFY	Контролируется работа с функциями проверки.
*SECVLDL	Контролируются изменения, вносимые в объекты контрольных списков.
*SERVICE	Контролируется работа со служебными средствами.
*SPLFDTA	Регистрируются действия, выполняемые над буферными файлами.
*SYSMGT	Регистрируется работа с функциями управления системами.

Ссылки, связанные с данной

“Планирование контроля действий” на стр. 278

Для контроля действий используются системные значения QAUDCTL (управление контролем), QAUDLVL (уровень контроля), QAUDLVL2 (расширение уровня контроля), а также параметр AUDLVL (контроль действий) из пользовательских профайлов.

Контроль за новыми объектами (QCRTOBJAUD)

Системное значение Контроль за новыми объектами (QCRTOBJAUD) позволяет определить значение контроля для нового объекта, если в качестве значения контроля по умолчанию для библиотеки или каталога нового объекта указано *SYSVAL.

Кроме того, системное значение QCRTOBJAUD представляет собой значение контроля объекта по умолчанию для новых документов, не находящихся в папке.

Например, для библиотеки CUSTLIB в CRTOBJAUD указано значение *SYSVAL. Значение QCRTOBJAUD - *CHANGE. При создании нового объекта в библиотеке CUSTLIB для него автоматически задается значение контроля *CHANGE. Значение контроля объекта можно изменить с помощью команды CHGOBJAUD или CHGAUD.

Примечание: Это ограниченное системное значение. Подробная информация об ограничении изменения системных значений защиты, а также полный список ограниченных системных значений приведены в главе Системные значения защиты.

Таблица 52. Для системного значения QCRTOBJAUD предусмотрены следующие значения:

*NONE	Контроль за объектом не ведется.
*NOTAVL	Означает, что системное значение недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение системному значению нельзя.

Таблица 52. Для системного значения QCRTOBJAUD предусмотрены следующие значения: (продолжение)

*USRPRF	Контроль за объектом основан на значении, указанном в пользовательском профайле, от имени которого пользователь обращается к объекту.
*CHANGE	Запись контроля заносится при каждом относящемся к защите изменении объекта.
*ALL	Запись контроля заносится для каждого относящегося к защите действия, изменяющего содержимое объекта. Кроме того, запись контроля заносится в случае относящегося к защите изменения содержимого объекта.

Рекомендуемое значение: Выбираемое значение зависит от конкретных требований к контролю. В разделе “Планирование контроля доступа к объектам” на стр. 304 приведена дополнительная информация о методах настройки контроля за объектами в системе. Значение контроля можно задавать на уровне каталогов - с помощью параметра CRTOBJAUD команды Создать каталог (CRTDIR) и значения *CRTOBJAUD команды Изменить атрибут (CHGATR). Кроме того, значение контроля можно изменить на уровне библиотеки с помощью команд CRTLIB и CHGLIB, в которых указан параметр CRTOBJAUD.

Глава 4. Пользовательские профайлы

Пользовательские профайлы - это мощный и гибкий инструмент. Правильная организация пользовательских профайлов поможет защитить систему и настроить ее для пользователей.

Описание:

Задача:

Создание и поддержка пользовательских профайлов и профайлов групп.

Средства для ее решения:

Команда Работа с пользовательскими профайлами (WRKUSRPRF)

Команда Изменить пользовательский контроль (CHGUSRAUD)

Права доступа:

Специальные права доступа *SECADM

Специальные права доступа *AUDIT для изменения пользовательского контроля

Запись в журнале:

AD - изменения пользовательского контроля

CO - создание пользовательского профайла

CP - изменения, внесенные в пользовательские профайлы

DO - удаление пользовательского профайла

ZC - изменения пользовательских профайлов, не связанные с защитой

Понятия, связанные с данным

“Пользовательские профайлы” на стр. 4

У каждого пользователя в системе i5/OS есть пользовательский профайл.

Роли пользовательских профайлов

Пользовательский профайл содержит пароли пользователя и список предоставленных пользователю специальных прав доступа и объектов, принадлежащих данному пользователю.

Пользовательский профайл выполняет следующие задачи в системе:

- Содержит информацию, относящуюся к защите и определяющую, каким образом пользователь входит систему, какие действия разрешено ему выполнять после входа в систему и каким образом эти действия контролируются.
- Содержит информацию, необходимую для настройки системы для работы пользователя.
- Играет роль инструмента управления и восстановления для операционной системы. Пользовательский профайл содержит информацию об объектах, принадлежащих пользователю, а также обо всех частных правах доступа к этим объектам.
- Идентифицирует задания пользователя и его вывод на принтер.

Если в системном значении Уровень защиты (QSECURITY) указан уровень 10, то система автоматически создает пользовательский профайл при входе нового пользователя в систему. В таблице “Значения по умолчанию для пользовательских профайлов” на стр. 337 раздела Приложение В, “Пользовательские профайлы, поставляемые IBM”, на стр. 337 приведены значения, присваиваемые при автоматическом создании пользовательского профайла.

Если в системном значении QSECURITY указан уровень защиты 20 и выше, то в систему может войти только пользователь с уже существующим пользовательским профайлом.

Профайлы групп

Профайл группы - это особый тип пользовательского профайла, предоставляющий одинаковые права доступа всем пользователям группы.

Профайл группы выполняет следующие две задачи:

Средство защиты

Профайл группы позволяет предоставить один и тот же набор прав доступа сразу нескольким пользователям - группе. Вы можете указывать права доступа к объекту или специальные права доступа в профайлах групп, вместо того чтобы предоставлять их каждому пользователю в отдельности. Каждый пользователь может входить не более чем в 16 профайлов групп.

Средство настройки

Профайл группы может применяться в качестве шаблона для создания отдельных пользовательских профайлов. Как правило, у пользователей, входящих в состав группы, схожие требования, например, им нужны одни и те же начальное меню и принтер по умолчанию. Эти параметры можно указать в профайле группы, а затем на его основе создать отдельные пользовательские профайлы.

Профайлы групп создаются так же, как и обычные пользовательские профайлы. Система распознает профайл группы, когда вы добавляете в него первого пользователя. После этого система задает в профайле информацию, указывающую на то, что это профайл группы. Кроме того, для профайла создается идентификационный номер группы (GID). Профайл можно сделать профайлом группы, задав при его создании параметр gid. В разделе “Планирование профайлов групп” на стр. 251 приведен пример создания профайла группы.

Поля параметров пользовательского профайла

В этом разделе описаны поля параметров пользовательского профайла, показанные в окне команды Создать пользовательский профайл.

При создании пользовательского профайла ему предоставляются следующие права доступа: *OBJMGT, *CHANGE. Эти права доступа необходимы для функций системы и их не следует удалять.

Для многих системных меню предусмотрены различные версии, называемые *уровнями поддержки*, соответствующие потребностям различных пользователей:

- Основной уровень поддержки, в котором приведен минимальный объем информации и не применяется техническая терминология.
- Промежуточный уровень поддержки, в котором приведена дополнительная информация и применяются техническая терминология.
- Расширенный уровень поддержки, в котором применяется техническая терминология и приведен максимальный объем информации, но информация о функциональных клавишах и опциях отображается не всегда.

В следующих разделах приведены названия полей пользовательского профайла, применяемые как на основном, так и на промежуточном уровнях поддержки.

Название поля

Название раздела соответствует имени поля, отображаемого в приглашении команды Создать пользовательский профайл, которое появляется при создании пользовательского профайла на промежуточном уровне поддержки или с помощью команды Создать пользовательский профайл (CRTUSRPRF).

Приглашение Добавить пользователя:

Таким образом имя поля отображается в меню Добавить пользователя и других меню пользовательского профайла на основном уровне поддержки. Меню основного уровня поддержки отображают набор полей пользовательского профайла. *Не показывается* означает, что поле не отображается в меню основного уровня поддержки. При создании пользовательского профайла с помощью меню Добавить пользователя для всех неотображаемых полей применяются значения по умолчанию.

Параметр CL:

Имя параметра CL применяется для поля в программе CL, либо при вводе команды пользовательского профайла без приглашения.

Длина:

Если в программе CL применяется команда Загрузить пользовательский профайл (RTVUSRPRF), то здесь указывается длина, применяемая для определения поля, связанного с параметром.

Права доступа:

Перечислены необходимые права доступа к объекту, если поле связано с отдельным объектом, таким как библиотека или программа. Эти права доступа требуются для указания объекта при создании или изменении пользовательского профайла. Для входа в систему от имени этого пользовательского профайла требуются данные права доступа. Например, для создания пользовательского профайла USERA с описанием задания JOB D1, требуются права доступа *USE к JOB D1. Для входа в систему от имени USERA необходимы права доступа *USE к JOB D1.

Кроме того, в каждом разделе приведены возможные значения для поля, а также рекомендуемые значения.

Пользовательский профайл

Имя пользовательского профайла необходимо для идентификации пользователя. Имя пользовательского профайла также называется ИД пользователя. Пользователь вводит имя в приглашение Пользователь меню Вход в систему.

Приглашение Добавить пользователя:

Пользователь (User)

Параметр CL:

USRPRF

Длина:

10

Длина имени пользовательского профайла не может превышать 10 символов. Допустимы следующие символы:

- Буквы (A - Z)
- Цифры (0 - 9)
- Специальные символы: #, \$, @ и подчеркивание (_).

Имя пользовательского профайла не может начинаться с цифры.

Notes:

- В меню Добавить пользователя максимальная длина имени пользователя ограничена 8 символами.
- Пользовательский профайл можно создать таким образом, что при входе в систему указывается ИД пользователя, состоящий только из цифр. Для создания подобного профайла укажите Q в качестве первого символа. Например, Q12345. При этом пользователь может войти в систему указав в приглашении *Пользователь* меню Вход в систему 12345 или Q12345.

Дополнительная информация о задании имен в системе приведена в разделе Программирование CL.

Рекомендации по присвоению имен пользовательским профайлам: В процессе задания имен для пользовательских профайлов учтите следующие особенности и рекомендации:

- Длина имени пользовательского профайла может составлять до 10 символов. Некоторые методы связи ограничивают ИД пользователя до восьми символов. Длина имени пользовательского профайла в меню Добавить пользователя также ограничена до восьми символов.
- Применяйте соглашение о присвоении имен, позволяющее легко запоминать ИД пользователей.
- В имени пользовательского профайла не учитывается регистр символов. Если в рабочей станции указать строчные буквы, то система автоматически преобразует в прописные буквы.
- В меню и списках, управляющих пользовательскими профайлами, они отображаются в алфавитном порядке.
- Не рекомендуется применять в именах пользовательских профайлов специальные символы. Специальные символы могут привести к неполадкам, связанным с раскладкой клавиатуры некоторых рабочих станций или версий языков лицензионных программ i5/OS.

Одна из стратегий присваивания имен пользовательским профайлам заключается в следующем: используются первые семь символов фамилии пользователя и первый символ его имен. Например:

Имя пользователя	Пользовательский профайл
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Harrisburg, Keith	HARRISBK
Jones, Sharon	JONESS
Jones, Keith	JONESK

Рекомендации по присвоению имен профайлам групп: Для того чтобы без затруднений отличать профайлы групп, рекомендуется применять соглашение о присвоении имен в системе. Например, все имена профайлов групп могут начинаться с одних и тех же символов, таких как GRP (для группы) или DPT (для отдела).

Пароль

Пароль применяется для проверки прав доступа пользователей при входе в систему. Для того чтобы войти в защищенную систему необходим ИД пользователя и пароль (в системном значении QSECURITY должно быть указано значение выше 20).

Приглашение Добавить пользователя:

Пароль

Параметр CL:

PASSWORD

Длина:

128

Максимальная длина пароля задается с помощью системного значения QPWDLVL. Если в QPWDLVL указано значение 0 или 1, то длина пароля не может превышать 10 символов. Если указано значение 2 или 3, то длина пароля ограничена 128 символами.

Если в системном значении Уровень пароля (QPWDLVL) указано значение 0 или 1, то правила определения паролей не отличаются от правил, применяемых для имен пользовательских профайлов. Указав в качестве первого символа пароля символ Q, за которым следует цифра, при входе в систему вы можете не указывать символ Q. Если в качестве пароля в окне Изменить пароль указана строка Q12345, то в окне Вход в систему можно указать 12345, либо Q12345. На уровне QPWDLVL 2 или 3 при входе в систему пользователь должен указать пароль полностью, т.е. если для пользовательского профайла указан пароль Q12345, в окне входа в

систему следует указать Q12345. На уровнях QPWDLVL 2 и 3 разрешены пароли, состоящие только из цифр. Для этого пароль пользовательского профайла должен создаваться как числовой.

Если в системном значении Уровень пароля (QPWDLVL) указано значение 2 или 3, в пароле учитывается регистр символов и поддерживаются все символы, включая пробел. Однако пароль не может начинаться со звездочки (*); кроме того, все конечные пробелы в пароле удаляются.

Примечание: Пароли можно создавать с помощью двухбайтовых символов. Однако с помощью пароля, содержащего двухбайтовые символы, вы не сможете войти в систему через меню входа в систему. Пароли, содержащие двухбайтовые символы, создаются с помощью команд CRTUSRPRF и CHGUSRPRF и могут передаваться системным API, поддерживающим параметр password.

Для хранения паролей в системе применяется одностороннее шифрование. Если пользователь забыл пароль, системный администратор с помощью команды Изменить пользовательский профайл (CHGUSRPRF) может задать временный пароль и указать, что срок его действия истек. При этом пользователю потребуется изменить его при следующем входе в систему.

- | С помощью системных значений можно контролировать состав паролей, указываемых пользователями.
- | Системные значения, связанные с составом пароля, применимы только в том случае, если пароль изменяется с помощью команды Изменить пароль (CHGPWD), опции Изменить пароль меню Поддержка или API QSYCHGPW. Пользователь не сможет указать с помощью команды CHGPWD, опции меню Поддержка или API QSYCHGPW пароль, совпадающий с именем пользовательского профайла, если выполнено одно из следующих условий.
- | • Системное значение QPWDRULES равно *PWDSYSVAL и системное значение Минимальная длина пароля (QPWDMINLEN) не равно 1.
- | • Системное значение QPWDRULES равно *PWDSYSVAL и системное значение Максимальная длина пароля (QPWDMAXLEN) не равно 10.
- | • Системное значение QPWDRULES равно *PWDSYSVAL и любое из прочих системных значений составления пароля отличается от значения по умолчанию.

Дополнительная информация о системных значениях, связанных с составом пароля, приведена в разделе “Системные значения, связанные с паролями” на стр. 49.

Таблица 53. Возможные значения для параметра PASSWORD:

*USRPRF	Пароль этого пользователя совпадает с именем пользовательского профайла. Если в системном значении Уровень пароля (QPWDLVL) указано значение 2 или 3, то пароль представляет собой имя пользовательского профайла, указанное прописными буквами. Например, для профайла JOHNDOE пароль будет JOHNDOE, а не johndoe.
*NONE	Данному пользовательскому профайлу пароль не присваивается. Вход в систему от имени этого пользовательского профайла запрещен. С помощью пользовательского профайла, для пароля которого указано значение *NONE, можно отправить на выполнение пакетное задание. Для этого необходимы соответствующие права доступа к пользовательскому профайлу.
<i>пароль-пользователя</i>	Символьная строка (не более 128 символов).

Рекомендации для паролей:

- Укажите пароль *NONE для профайла группы. С помощью такого профайла нельзя войти в систему.
- При создании отдельных пользовательских профайлов задайте начальный пароль и укажите, что его необходимо изменить при следующем входе пользователя в систему (значение *YES для параметра истечения срока действия пароля). Пароль пользователя по умолчанию должен совпадать с именем пользовательского профайла.

- Если при создании пользовательских профайлов используются простые пароли и пароли по умолчанию, убедитесь, что пользователь немедленно входит в систему. Если пользователь входит в систему через некоторое время, укажите для состояния пользовательского профайла значение *DISABLED. Измените состояние пользовательского профайла на *ENABLED непосредственно перед входом пользователя в систему. Это позволит защитить новый пользовательский профайл от несанкционированного использования.
- Применяйте системные значения, ограничивающие состав паролей. Они не позволяют пользователям указывать слишком простые пароли.
- Некоторые способы связи предусматривают отправку паролей между системами и ограничивают длину паролей, а также допустимые символы. Системное значение QPWDMAXLEN или QPWDRULES позволяет ограничить длину паролей, если система обменивается данными с другими системами. На уровне паролей 0 и 1 системное значение QPWDLMTCHR позволяет указать символы, которые запрещено применять в паролях.

Ограничить срок действия пароля

Поле *Ограничить срок действия пароля* позволяет администратору защиты указать в пользовательском профайле, что срок действия пароля истек и его необходимо изменить при следующем входе в систему.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

PWDEXP

Длина:

4

После изменения пароля это значение автоматически изменяется на *NO. Пароль можно изменить в процессе входа в систему с помощью команд CHGPWD или CHGUSRPRF, либо API QSYCHGPW.

С помощью этого поля администратор защиты может присвоить новый пароль, если пользователь забыл текущий пароль. При этом, так как пользователь должен изменить пароль при следующем входе в систему, администратор защиты не сможет войти в систему от имени этого пользователя.

В случае истечения срока действия пароля пользователя при входе в систему выдается соответствующее сообщение (см. “Срок действия пароля” на стр. 96). При этом пользователь может назначить новый пароль, нажав клавишу Enter, либо отменить вход в систему, нажав клавишу F3 (Выход). Для изменения пароля отображается меню Изменить пароль и выполняется проверка нового пароля.

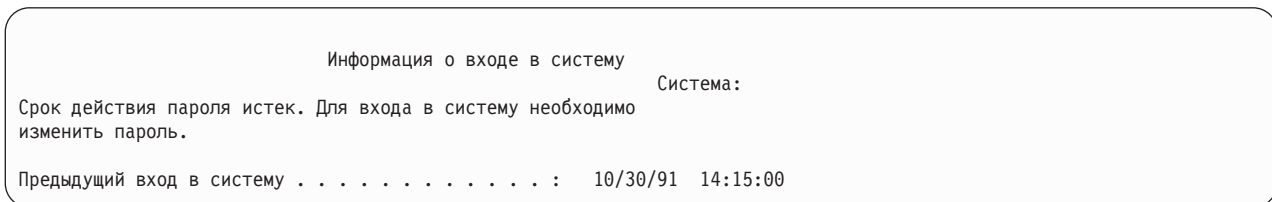


Рисунок 1. Сообщение об истечении срока действия пароля

Таблица 54. Возможные значения для параметра PWDEXP:

*NO:	Для пароля не указывается, что его срок действия истек.
*YES:	Позволяет указать, что срок действия пароля истек.

Рекомендации: Ограничение срока действия пароля необходимо, если вы создаете новые пользовательские профайлы или указываете для пользователей временные пароли.

Состояние

Значение поля *Состояние* указывает, разрешено ли применять профайл для входа в систему. Если для состояния профайла указано значение *ENABLED, то вход в систему с помощью этого профайла разрешен. В противном случае, пользователь с правами доступа должен включить этот профайл для того, чтобы он стал доступным для входа в систему.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

STATUS

Длина:

10

Включить отключенный профайл можно с помощью команды CHGUSRPRF. Для изменения состояния профайла необходимы специальные права доступа *SECADM и права доступа *OBJMGT и *USE к этому профайлу. В разделе “Включение пользовательского профайла” на стр. 129 приведен пример программы с принимаемыми правами доступа, которая позволяет оператору включить профайл.

Система может отключить пользовательский профайл после некоторого числа недопустимых попыток входа в систему от имени этого профайла в соответствии с параметрами системных значений QMAXSIGN и QMAXSGNACN.

Профайл QSECOFR (системный администратор) позволяет войти в систему с консоли даже в том случае, если для него указано состояние *DISABLED. Если пользовательский профайл QSECOFR будет отключен, войдите в систему от имени QSECOFR с помощью консоли и введите CHGUSRPRF QSECOFR STATUS(*ENABLED).

Таблица 55. Возможные значения для параметра STATUS:

*ENABLED	С помощью этого профайла можно войти в систему.
*DISABLED	Вход с систему с помощью этого профайла запрещен до тех пор, пока пользователь с правами доступа не изменит его состояние.

Рекомендации: Для того чтобы запретить вход в систему с помощью пользовательского профайла, укажите для его состояния значение *DISABLED. Например, рекомендуется отключать профайлы пользователей, которые будут отсутствовать в течение длительного времени.

Класс пользователя

Класс пользователя позволяет управлять опциями, доступными для пользователя в меню i5/OS. Это упрощает контроль за доступом пользователя к некоторым системным функциям.

Приглашение Добавить пользователя:

Тип пользователя

Параметр CL:

USRCLS

Длина:

10

Это связано не только с ограничением использования команд. Поле *Ограничить возможности* позволяет указать, разрешено ли пользователю вводить команды. Класс пользователя не применим для ограничения опций, доступных в меню других лицензионных программ.

Класс пользователя и системное значение Уровень защиты (QSECURITY) определяют специальные права доступа пользователя, если они не были указаны при создании пользовательского профайла.

Возможные значения для USRCLS: В таблице Табл. 56 приведены возможные классы пользователей с соответствующими специальными правами доступа. В записях может быть указано, что права доступа предоставляются только на уровнях 10 и 20, на всех уровнях защиты, либо не предоставляются.

По умолчанию для класса пользователя применяется значение *USER.

Таблица 56. Специальные права доступа по умолчанию для класса пользователя

Специальные права доступа	Классы пользователей				
	*SECOFR	*SECADM	*PGMR	*SYSOPR	*USER
*ALLOBJ	Все	10 или 20	10 или 20	10 или 20	10 или 20
*SECADM	Все	Все			
*JOBCTL	Все	10 или 20	10 или 20	Все	
*SPLCTL	Все				
*SAVSYS	Все	10 или 20	10 или 20	Все	10 или 20
*SERVICE	Все				
*AUDIT	Все				
*IOSYSCFG	Все				

Рекомендации: Большинству пользователей не требуются выполнять системные функции. Для класса пользователя рекомендуется применять значение *USER, если пользователю не требуется выполнять системные функции.

Уровень поддержки

Поле *Уровень поддержки* позволяет указать уровень поддержки по умолчанию при создании пользовательского профайла. На платформе System i существуют три уровня поддержки: основной, промежуточный и расширенный.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

ASTLVL

Длина:

10

Для каждого пользователя система отслеживает последний уровень поддержки, используемый в системном меню, для которого указано несколько уровней поддержки. Этот уровень применяется в следующем сеансе работы с этим меню. В активном задании пользователь может изменить уровень поддержки для меню или группы связанных меню с помощью клавиши F21 (Выбрать уровень поддержки). Новый уровень поддержки для этого меню сохраняется вместе с информацией о пользователе.

Указав уровень поддержки в команде с помощью параметра ASTLVL, вы не изменяете уровень поддержки, сохраненный для соответствующего меню в информации о пользователе.

Если уровень поддержки пользовательского профайла изменен с помощью команды CHGUSRPRF или Изменить профайл (CHGPRF), то новое значение заменяет старый уровень поддержки, сохраненный для всех меню.

Например, предположим, что пользовательский профайл USERA создан с уровнем поддержки по умолчанию (основной). В таблице Табл. 57 на стр. 85 показано, будет ли пользователю доступно меню Работа с пользовательскими профайлами или Работа с регистрацией пользователя, в зависимости от различных опций. Кроме того, в таблице показано, изменяет ли система версию меню, сохраненную в

профайле USERA.

Таблица 57. Как сохраняется и изменяется уровень поддержки

Действие	Версия показанного меню	Версия сохраненного меню
Выполнение команды WRKUSRPRF	Работа с регистрацией пользователей, меню	Не изменяется (основной уровень поддержки)
Нажатие клавиши F21 и выбор промежуточного уровня поддержки в меню Работа с регистрацией пользователя.	Меню Работа с пользовательскими профайлами	Изменяется на промежуточный уровень поддержки
Выполнение команды WRKUSRPRF	Меню Работа с пользовательскими профайлами	Не изменяется (промежуточный)
Выбор опции Работа с регистрацией пользователя в меню Настройка.	Меню Работа с пользовательскими профайлами	Не изменяется (промежуточный)
Ввод CHGUSRPRF USERA ASTLVL(*BASIC)		Изменяется на основной уровень поддержки
Выполнение команды WRKUSRPRF	Работа с регистрацией пользователей, меню	Не изменяется (основной)
Ввод WRKUSRPRF ASTLVL(*INTERMED)	Меню Работа с пользовательскими профайлами	Не изменяется (основной)

Примечание: Поле *Опция пользователя* также позволяет управлять способом отображения системных меню. Это поле описано на странице “Опции пользователя” на стр. 113.

Таблица 58. Возможные значения параметра ASTLVL

*SYSVAL	Применяется уровень поддержки, указанный в системном значении QASTLVL.
*BASIC	Применяется пользовательский интерфейс Операционной поддержки.
*INTERMED	Применяется системный интерфейс.
*ADVANCED	Применяется экспертный системный интерфейс. Для отображения дополнительных записей списка в некоторых случаях не показываются номера опций и функциональные клавиши. Если для команды не предусмотрен расширенный уровень (*ADVANCED), то используется промежуточный (*INTERMED).

Текущая библиотека

Текущая библиотека - это первая библиотека, в которой ищутся объекты при запросе пользователя. Если при создании объектов пользователь указывает параметр *CURLIB, то они добавляются в текущую библиотеку.

Приглашение Добавить пользователя:

Библиотека по умолчанию

Параметр CL:

CURLIB

Длина:

10

Права доступа

*USE

Текущая библиотека автоматически добавляется в список библиотек пользователя при входе в систему. Ее не требуется включать в исходный список библиотек описания задания пользователя.

Пользователь не может изменить текущую библиотеку, если в поле пользовательского профайла *Ограничить возможности* указано значение *YES или *PARTIAL.

Более подробная информация о работе со списками библиотек и текущей библиотекой приведена в разделе “Списки библиотек” на стр. 218.

Таблица 59. Возможные значения для CURLIB:

*CRTDFT	Текущая библиотека для пользователя не задана. Если при создании объекта в команде указан параметр *CURLIB, то в качестве текущей библиотеки по умолчанию применяется QGPL.
имя-текущей-библиотеки	Имя библиотеки.

Рекомендации: Поле *Текущая библиотека* позволяет указать, разрешено ли пользователям помещать новые объекты, такие как программы Query. Поле *Ограничить возможности* позволяет запретить пользователям изменять текущую библиотеку.

Начальная программа

Вы можете указать имя программы, вызываемой при входе в систему. Такая программа называется начальной программой. Эта программа выполняется до начального меню, если оно показывается.

Приглашение Добавить пользователя:

Программа, вызываемая при входе в систему

Параметр CL:

INLPGM

Длина:

10 (имя программы) 10 (имя библиотеки)

Права доступа:

*USE для программы, *EXECUTE для библиотеки

Если в поле пользовательского профайла *Ограничить возможности* указано значение *YES или *PARTIAL, то пользователь не может задать начальную программу или меню Вход в систему.

Начальная программа вызывается только в том случае, если для пользователя в качестве программы выполнения указана QCMD или QCL. Дополнительная информация о последовательности обработки при входе в систему приведена в разделе “Запуск интерактивного задания” на стр. 209.

Начальная программа предназначена для следующих целей:

- Для того, чтобы ограничить функции, доступные пользователю.
- Для выполнения начальных действий, таких как открытие файлов или создание списка библиотек, при первом входе пользователя в систему.

Начальной программе нельзя передавать параметры. Если начальная программа не может быть выполнена, то пользователь не сможет войти в систему.

Таблица 60. Возможные значения для INLPGM:

*NONE	Начальная программа не вызывается. Если в параметре Начальная программа (INLMNU) указано имя, то выводится соответствующее меню.
имя-программы	Имя программы, вызываемой при входе пользователя в систему.

Таблица 61. Возможные значения для библиотеки INLPGM:

*LIBL	Для поиска программы применяется список библиотек. Если список библиотек указан в описании задания пользовательского профайла, то применяется этот список. Если в описании задания для начального списка библиотек указано значение *SYSVAL, то применяется системное значение QUSRLIBL.
*CURLIB	Поиск программы выполняется в текущей библиотеке, указанной в пользовательском профайле. Если текущая библиотека не указана, то применяется QGPL.
<i>библиотека</i>	Имя библиотеки, в которой расположена программа.

Начальное меню

При необходимости вы можете указать имя меню, которое будет отображаться при входе в систему. Начальное меню отображается после выполнения начальной программы. Начальное меню вызывается только в том случае, если для пользователя в качестве программы выполнения указана QCMD или QCL.

Приглашение Добавить пользователя:

Первое меню

Параметр CL:

INLMNU

Длина:

10 (имя меню) 10 (имя библиотеки)

Права доступа

*USE для меню, *EXECUTE для библиотеки

Для того чтобы выполнялась только начальная программа укажите для начального меню значение *SIGNOFF.

Если в поле пользовательского профайла Ограничить возможности указано значение *YES, то пользователь не может задать другое начальное меню для меню Вход в систему. Если пользователю разрешено указывать начальное меню, то указанное меню переопределяет меню, заданное в пользовательском профайле.

Таблица 62. Возможные значения для параметра MENU:

MAIN	Будет показано Главное меню System i.
*SIGNOFF	После выполнения начальной программы сеанс работы с системой завершается. Это значение позволяет запускать только одну программу.
<i>имя-меню</i>	Имя меню, вызываемого при входе пользователя в систему.

Таблица 63. Возможные значения для библиотеки MENU:

*LIBL	Для поиска меню применяется список библиотек. Так как меню вызывается после выполнения начальной программы, то записи добавленные этой программой в список библиотек также участвуют в поиске.
*CURLIB	Меню выбирается с помощью текущей библиотеки задания. Если текущая библиотека не существует в списке библиотек, применяется QGPL.
<i>библиотека</i>	Имя библиотеки, в которой расположено меню.

Ограничить возможности

С помощью поля Ограничить возможности вы можете ограничить доступ пользователя к командной строке на ввод команд и переопределение начальной программы, начального меню, текущей библиотеки и

программы обработки клавиши Attention, указанной в пользовательской профайле. Это поле представляет собой инструмент, позволяющий ограничить возможности пользователя по изменению параметров системы.

Приглашение Добавить пользователя:

Ограничить доступ к командной строке

Параметр CL:

LMTCPB

Длина:

10

Пользователь, для ограничены функции, может запускать только те команды, которые разрешено запускать таким пользователям. Параметр ALWLMTUSR(*YES) указан для следующих поставляемых команд IBM:

- Выйти из системы (SIGNOFF)
- Отправить сообщение (SNDMSG)
- Показать сообщения (DSPMSG)
- Показать задание (DSPJOB)
- Показать протокол задания (DSPJOBLOG)
- Запустить PC Organizer (STRPCO)
- Работа с сообщениями (WRKMSG)

Поле пользовательского профайла Ограничить возможности и параметр команд ALWLMTUSR применимы только к командам, запускаемым с помощью командной строки, меню Ввод команды, FTP, REXEC, API QCAPCMD или опции из меню группировки команд. Пользователям разрешены следующие действия:

- Выполнение команд в программах CL, запускающих команды в результате выбора опции меню.
- Выполнение удаленных команд с помощью приложений

Пользователю с ограниченными возможностями можно разрешить запуск дополнительных команд, либо удалить их из списка, изменив для команды параметр ALWLMTUSR. Для этого воспользуйтесь командой Изменить команду (CHGCMD). В случае создания собственных команд параметр ALWLMTUSR можно указать в команде Создать команду (CRTCMD).

Возможные значения: В таблице Табл. 64 показаны возможные значения для поля Ограничить возможности, а также функции, разрешенные для каждого значения.

Таблица 64. Функции, разрешенные для значений поля Ограничить возможности

Функция	*YES	*PARTIAL	*NO
Изменение начальной программы	Нет	Нет	Да
Изменение начального меню	Нет	Да	Да
Изменить текущую библиотеку	Нет	Нет	Да
Изменение программы Attention	Нет	Нет	Да
Ввести команды	Несколько ¹	Да	Да
¹ Разрешены по умолчанию следующие команды: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, STRPCO, WRKMSG. Пользователь не может просмотреть командную строку из меню с помощью клавиши F9.			

Рекомендации: Применение начального меню, ограничение использования командной строки и предоставление доступа к меню позволяют создать среду для пользователя, которому не нужен доступ к системным функциям.

Понятия, связанные с данным

“Планирование меню” на стр. 240

Меню являются хорошим способом предоставления управляемого доступа к системе. Они позволяют предоставить пользователю доступ к фиксированному набору строго контролируемых функций, ограничив возможности пользователя и задав начальное меню в пользовательском профайле.

Описание

Текст, указанный в пользовательском профайле, позволяет описать пользовательский профайл или его предназначение.

Приглашение **Добавить пользователя:**

Описание пользователя

Параметр **CL:**

TEXT

Длина:

50

Для пользовательских профайлов это должна быть идентификационная информация, такая как имя пользователя или название отдела. Для профайла группы должна быть указана информация о группе, такая как входящие в нее отделы.

Таблица 65. Возможные значения для текста:

*BLANK:	Текст не указан.
<i>описание</i>	Укажите описание, длиной до 50 символов.

Рекомендации: Поле *Текст* усекается во многих системных меню. Рекомендуется указывать наиболее важную идентификационную информацию в начале поля.

Специальные права доступа

Специальные права доступа позволяют указать действия над ресурсами системы, которые разрешено выполнять пользователю. Пользователю можно предоставить специальные права доступа одного или двух типов.

Приглашение **Добавить пользователя:**

Не показывается

Параметр **CL:**

SPCAUT

Длина:

100 (10 символов для специальных прав доступа)

Права доступа:

Для того чтобы предоставить пользовательскому профайлу специальные права доступа вы должны обладать этими правам доступа.

Таблица 66. Возможные значения для параметра SPCAUT:

*USRCLS	<p>Специальные права доступа предоставляются в соответствии с классом пользователя (USRCLS), указанным в пользовательском профайле, и системным значением Уровень защиты (QSECURITY). Если для пользователя указано значение *USRCLS, то ему нельзя предоставить дополнительные специальные права доступа.</p> <p>Если указать значение *USRCLS при создании или изменении пользовательского профайла, система автоматически исправляет специальные права доступа. При просмотре пользовательских профайлов нельзя определить, каким образом были добавлены специальные права доступа: по отдельности или в соответствии с классом пользователя.</p> <p>В таблице Табл. 56 на стр. 84 перечислены специальные права доступа по умолчанию, предоставляемые всем классам пользователей.</p>
*NONE	Специальные права доступа не предоставляются.
<i>специальные права доступа</i>	Укажите один или несколько типов специальных права доступа.

***ALLOBJ, специальные права доступа**

Специальные права доступа ко всем объектам (*ALLOBJ) позволяют пользователю получить доступ ко всем ресурсам системы, независимо от наличия частных прав доступа.

Специальные права доступа *ALLOBJ позволяют получить доступ к объекту даже в том случае, если к этому объекту пользователь обладает правами доступа *EXCLUDE.

Опасность для защиты: Специальные права доступа *ALLOBJ предоставляют пользователю права доступа ко всем ресурсам системы. Пользователь может просмотреть, изменить и удалить любой объект. Кроме того, он может предоставить права доступа к объектам другим пользователям.

Пользователь, обладающий правами доступа *ALLOBJ, не может непосредственно выполнять операции, требующие других специальных прав доступа. Например, специальные права доступа *ALLOBJ не позволяют создать другой пользовательский профайл, так как для этого необходимы специальные права доступа *SECADM. Однако с помощью специальных прав доступа можно отправить на выполнение пакетное задание, которое будет выполнено от имени пользовательского профайла, обладающего необходимыми специальными правами доступа. Предоставление специальных прав доступа *ALLOBJ позволяет пользователю получить доступ ко всем функциям системы.

Специальные права доступа *SECADM

Специальные права доступа Администратора защиты (*SECADM) позволяют создавать, изменять и удалять пользовательские профайлы.

Пользователь со специальными правами доступа *SECADM может выполнять следующие действия:

- Добавлять пользователей в системный каталог рассылки.
- Просматривать права доступа к документам и папкам.
- Добавлять в систему коды доступа и удалять их.
- Предоставлять пользователю коды доступа и аннулировать их.
- Разрешать и запрещать пользователям работать от имени других пользователей.
- Удалять документы и папки.
- Удалять списки документов.
- Изменять списки рассылки, созданные другими пользователями.

Специальные права доступа *SECADM могут быть предоставлены только пользователем, обладающим правами доступа *ALLOBJ и *SECADM.

Специальные права доступа *JOBCTL

Пользователь, обладающий специальными правами доступа *JOBCTL, может изменять приоритет заданий и печати, завершать задания до их выполнения и удалять вывод перед тем, как он будет распечатан. Кроме того, с помощью специальных прав доступа *JOBCTL пользователь может получить доступ к конфиденциальному буферизованному выводу, если для очередей вывода указан параметр OPRCTL(*YES).

Специальные права доступа на управление заданием (*JOBCTL) позволяют пользователю выполнять следующие действия:

- Изменять, удалять, блокировать и разблокировать все файлы, расположенные в любых очередях вывода, для которых указан параметр OPRCTL(*YES).
- Просматривать, отправлять и копировать файлы, расположенные в любых очередях вывода, для которых указаны параметры DSPDTA(*YES или *NO) и OPRCTL(*YES).
- Блокировать, разблокировать и очищать очереди заданий, для которых указан параметр OPRCTL(*YES).
- Блокировать, разблокировать и очищать очереди вывода, для которых указан параметр OPRCTL(*YES).
- Блокировать, разблокировать, изменять и отменять задания других пользователей.
- Запускать, изменять, завершать, блокировать и разблокировать загрузчики, если для очереди вывода указан параметр OPRCTL(*YES).
- Изменять атрибуты выполняющихся заданий, таких как печать вывода задания.
- Останавливать подсистемы.
- Выполнять загрузку начальной программы (IPL).

Защита вывода на принтер и очередей вывода подробно описана в разделе “Печать” на стр. 221.

Для изменения приоритета (JOBPTY) и приоритета вывода (OUTPTY) собственного задания специальные права доступа не требуются. Специальные права доступа *JOBCTL необходимы для изменения приоритета выполнения задания (RUNPTY).

Диапазон изменения приоритета задания и приоритета вывода задания пользователя ограничен параметром Ограничение приоритета (PTYLMT), указанным в пользовательском профайле, от имени которого работает пользователь.

Риск: Неправильное использование специальных прав доступа *JOBCTL может отрицательно сказаться на отдельных заданиях и привести к общему снижению производительности системы.

Специальные права доступа *SPLCTL

Специальные права доступа на управление буфером (*SPLCTL) позволяют выполнять все функции, связанные с управлением буфером, такие как изменение, удаление, просмотр, блокирование и разблокирование буферных файлов.

Пользователь, обладающий этими правами доступа, может выполнять эти функции во всех очередях вывода, независимо от прав доступа и значения параметра OPRCTL, указанных для очереди вывода. Кроме того, специальные права доступа *SPLCTL позволяют управлять очередями заданий, включая блокирование, разблокирование и очистку очередей заданий. Пользователь, обладающий этими правами доступа, может выполнять эти функции во всех очередях заданий, независимо от прав доступа и значения параметра OPRCTL, указанных для очередей заданий.

Опасность для защиты: Пользователь, обладающий специальными правами доступа *SPLCTL, может выполнить любую операцию над любым буферным файлом системы. Конфиденциальные буферные файлы нельзя защитить от пользователя, обладающего специальными правами доступа *SPLCTL.

Специальные права доступа *SAVSYS

Специальные права доступа на сохранение системы (*SAVSYS) позволяют сохранять, восстанавливать и освобождать память для всех объектов системы, независимо от прав доступа к этим объектами.

Опасность для защиты: Пользователь, обладающий специальными правами доступа *SAVSYS может выполнять следующие действия:

- Сохранить объект и восстановить его в другой системе.
- Сохранить объект и просмотреть данные с магнитной ленты.
- Сохранить объект и освободить память, тем самым удаляя данные объекта.
- Сохранить документ и удалить его.

Специальные права доступа *SERVICE

Служебные права доступа (*SERVICE) позволяют запустить Системный инструментарий с помощью команды STRSST. С его помощью пользователь, обладающий правами доступа *USE к программе, может отладить ее и выполнить служебные функции просмотра и изменения. Он также поддерживает функции трассировки.

Для создания дампа права доступа *SERVICE не требуются.

Опасность для защиты: Пользователь, обладающий специальными правами доступа *SERVICE, с помощью служебных функций может просматривать и изменять конфиденциальную информацию. Для изменения информации с помощью служебных функций необходимы специальные права доступа *ALLOBJ.

Для выполнения служебной трассировки пользователям не обязательно предоставлять специальные права доступа *SERVICE. Такой подход позволяет максимально уменьшить риск, связанный с трассировкой команд. Таким образом, выполнять команды трассировки, позволяющие получить доступ к конфиденциальным данным, смогут только заданные пользователи. У пользователя должны быть права доступа к команде, а также специальные права доступа *SERVICE или права доступа к функции i5/OS Служебная трассировка, предоставленные с помощью функции Администрирование приложений Навигатора System i. Внести изменения в список пользователей, которым разрешено выполнять операции трассировки, можно с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав в ней в качестве ИД функции QIBM_SERVICE_TRACE.

Таким способом можно предоставить права доступа к следующим командам:

STRCMNTRC	Начать трассировку средств связи
ENDCMNTRC	Завершить трассировку средств связи
PRTCMNTRC	Распечатать трассировку средств связи
DLTCMNTRC	Удалить трассировку средств связи
CHKCMNTRC	Проверить трассировку средств связи
TRCCNN	Трассировать соединение (см. "Предоставление доступа к трассировке")
TRCINT	Внутренняя трассировка
STRTRC	Начать трассировку задания
ENDTRC	Завершить трассировку задания
PRTTRC	Распечатать трассировку задания
DLTRC	Удалить трассировку задания
TRCTCPAPP	Трассировать приложение TCP/IP
WRKTRC	Работа с трассировками

Примечание: Для изменения данных с помощью служебных функций необходимы права доступа *ALLOBJ.

Предоставление доступа к трассировке:

Команды трассировки, такие как TRCCNN (Трассировать соединение), представляют собой мощные служебные средства. Не рекомендуется предоставлять доступ к ним пользователям, которым необходимы другие служебные средства и отладочные средства.

Для того чтобы ограничить доступ к этим командам трассировки для пользователей, не обладающих правами доступа *SERVICE, выполните следующие действия:

1. В окне Навигатора System i откройте папку Пользователи и группы.
2. Выберите **Все пользователи** для просмотра списка пользовательских профайлов.
3. Правой кнопкой мыши щелкните на пользовательском профайле, который необходимо изменить.
4. Выберите пункт **Свойства**.
5. Нажмите кнопку **Возможности**.
6. Откройте вкладку Приложения.
7. Выберите **Права доступа**.
8. Выберите вкладку **Приложения хоста**.
9. Выберите **Операционная система**.
10. Выберите **Служба**.
11. С помощью переключателя предоставьте или аннулируйте доступ к команде трассировки.

Предоставлять пользователям доступ к командам трассировки можно также с помощью команды Изменить права доступа к функции (CHGFCNUSG). Введите CHGFCNUSG FCNID(QIBM_SERVICE_TRACE) USER(пользовательский_профайл) USAGE(*ALLOWED).

Специальные права доступа *AUDIT

Специальные права доступа на контроль (*AUDIT) позволяют просмотреть и изменить параметры контроля.

Пользователь с правами *AUDIT может выполнить следующие задачи:

- Изменить и просмотреть системные значения, управляющие контролем.
- Изменить контроль объектов с помощью команд CHGOBJAUT, CHGDLOAUD и CHGAUD.
- Изменить пользовательский контроль с помощью команды CHGUSRAUD.
- Просмотреть значения контроля для объекта.
- Просмотреть значения контроля для пользовательского профайла.
- Выполнить некоторые команды сервисных средств (например, PRTADPOBJ).

Опасность для защиты: Пользователь, обладающий специальными правами доступа *AUDIT, может остановить и запустить контроль системы, а также запретить контроль некоторых действий. Если контроль некоторых событий, связанных с защитой, важен для системы, рекомендуется тщательно проверять и отслеживать применение специальных прав доступа *AUDIT.

Для того чтобы обычный пользователь не мог видеть информацию контроля, ограничьте доступ к следующей информации:

- Журнал контроля (QAUDJRN)
- Другие журналы, содержащие информацию контроля
- Файлы сохранения, файлы вывода, буферные файлы и напечатанный вывод, содержащие информацию контроля

Примечание: Специальные права доступа *AUDIT могут быть предоставлены только пользователем, обладающим правами доступа *ALLOBJ, *SECADM и *AUDIT.

Специальные права доступа *IOSYSCFG

Специальные права доступа к конфигурации системы (*IOSYSCFG) позволяют пользователю вносить изменения в конфигурацию системы. Например, специальные права доступа позволяют добавить или удалить информацию о конфигурации средств связи, работать с серверами TCP/IP и настроить сервер соединения с Internet (ICS). Специальные права доступа *IOSYSCFG необходимы для работы с большинством команд по настройке средств связи.

Рекомендации по работе со специальными правами доступа: Предоставление специальных прав доступа пользователям связано с риском нарушения защиты системы. Тщательно оцените потребность каждого пользователя в специальных правах доступа. Отслеживайте пользователей, обладающих специальными правами доступа и периодически пересматривайте их потребности в этих правах доступа.

Кроме того, рекомендуется контролировать следующие возможности пользовательских профайлов и программ:

- Могут ли пользователи, обладающие специальными правами доступа, отправлять задания на выполнение.
- Могут ли программы, созданные этими пользователями, принимать права доступа владельца программы.

Программы могут принимать специальные права доступа *ALLOBJ владельца в следующих случаях:

- Программы созданы пользователями, обладающими специальными правами доступа *ALLOBJ.
- При создании программы указан параметр USRPRF(*OWNER).

Специальная среда

Пользователь может работать в среде System i5, System/36 или System/38. При входе в систему среда пользователя определяется с помощью программы выполнения и специальной среды.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

SPCENV

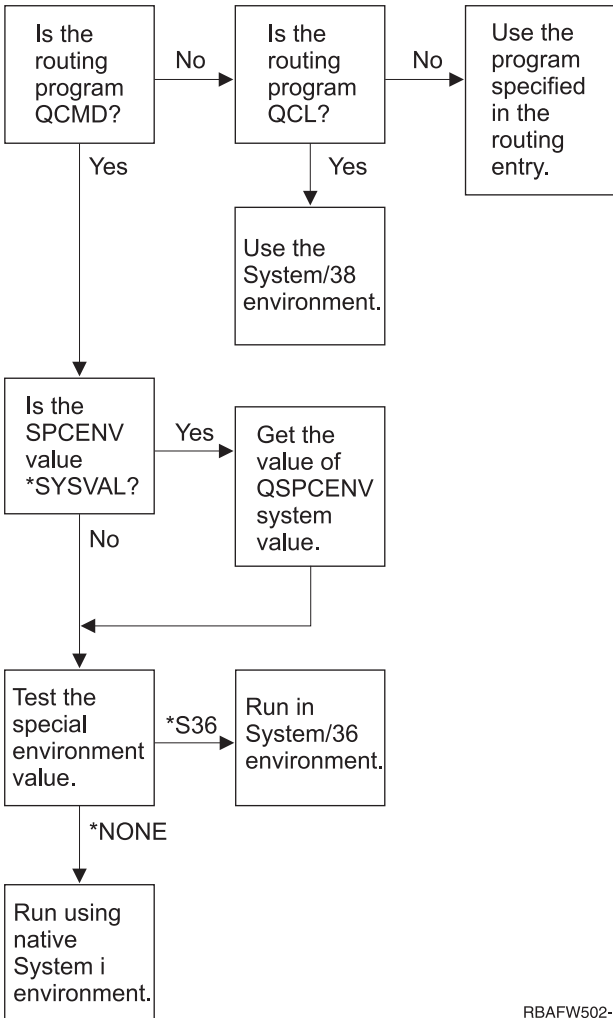
Длина:

10

Таблица 67. Возможные значения для параметра SPCENV:

*SYSVAL	Для определения среды при входе пользователя в систему применяется системное значение QSPCENV, если в качестве программы выполнения указана QCMD.
*NONE	Пользователь работает в среде System i5.
*S36	Пользователь работает в среде System/36, если в качестве программы выполнения указана QCMD.

Рекомендации: Если пользователь работает как с приложениями System i, так и с приложениями System/36, то рекомендуется перед запуском приложений System/36 выполнять команду Запуск System/36 (STRS36), а не указывать среду System/36 в пользовательском профайле. Это позволит обеспечить более высокую производительность для приложений System i.



RBAFW502-2

Рисунок 2. Описание специальной среды

Описание специальной среды в рис. 2

Система определяет, указана ли к качестве программы выполнения QCMD. Если нет, то проверяется программа QCL. Если в качестве программы выполнения указана QCL, то применяется специальная среда System/38. В противном случае система применяет программу, указанную в записи о выполнении.

Если в качестве программы выполнения указана QCMD, то проверяется системное значение SPCENV. Если оно указано, то проверяется значение системного значения QSPCENV. Если системное значение SPCENV не указано, то проверяется значение специальной среды.

Если в значении специальной среды указано *S36, запускается специальная среда System/36. Если указано значение *NONE, то система запускает стандартную среду System i.

Показать информацию о входе в систему

Меню Информация о входе в систему представляет собой средство, позволяющее пользователям обнаружить попытки несанкционированного использования их пользовательских профайлов. Поле Показать информацию о входе в систему задает необходимость отображения меню Информация о входе в систему в начале сеанса работы с системой.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

DSPSGNINF

Длина:

7

- На рисунке рис. 3 показано это меню. Информация об истечении срока действия пароля показывается только в том случае, если до истечения срока действия пароля осталось менее допустимого числа дней.

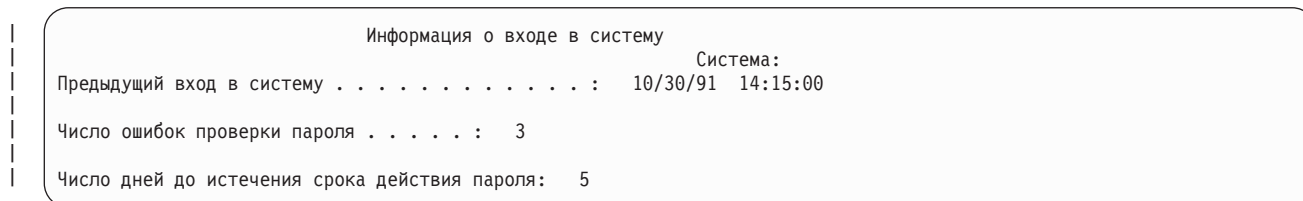


Рисунок 3. Меню Информация о входе в систему

Таблица 68. Возможные значения для DSPSGNINF:

*SYSVAL	Применяется системное значение QDSPSGNINF.
*NO	Меню Информация о входе в систему не отображается.
*YES	Меню Информация о входе в систему отображается.

Рекомендации: Это меню рекомендуется показывать всем пользователям. Пользователи, обладающие специальными правами доступа или правами доступа к особо важным объектам, должны проверять с помощью этого меню возможные попытки использования их профайлов.

Срок действия пароля

Срок действия пароля задает число дней, в течение которых можно использовать пароль.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

PWDEXPITV

Длина:

5,0

В случае истечения срока действия пароля при входе в систему пользователю выдается соответствующее сообщение. При этом пользователь может назначить новый пароль, нажав клавишу Enter, либо отменить вход в систему, нажав клавишу F3 (Выход). Для изменения пароля отображается меню Изменить пароль и выполняется проверка нового пароля. На рисунке “Срок действия пароля” приведен пример сообщения об истечении срока действия пароля.

Таблица 69. Возможные значения для параметра PWDEXPITV:

*SYSVAL	Применяется системное значение QPWDEXPITV.
*NOMAX	Смена пароля не требуется.
<i>срок-действия-пароля</i>	Укажите число от 1 до 366.

Рекомендации: Укажите в системном значении QPWDEXPITV срок действия от 60 до 90 дней. Для пользовательских профайлов со специальными правами доступа *SERVICE, *SAVSYS, *SECADM или *ALLOBJ рекомендуется указывать меньший срок действия паролей в поле Срок действия пароля.

Блокировка изменения пароля

Параметр Блокировка изменения пароля задает время, в течение которого запрещено изменение пароля после предыдущего изменения.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

PWDCHGBLK

Длина:

10

Этот параметр не ограничивает изменения пароля командой Изменить пользовательский профайл (CHGUSRPRF). Кроме того, этот параметр не учитывается, если значение Ограничить срок действия пароля (PWDEXP) пользовательского профайла равно *YES. Тем самым администратор защиты может создать пользовательский профайл с просроченным паролем и тем не менее разрешить однократный вход в систему для смены пароля.

Таблица 70. Возможные значения для параметра PWDCHGBLK:

*SYSVAL	Применяется системное значение QPWDCHGBLK.
*NONE	Значение пароля может быть изменено в любой момент.
1 - 99	Пароль можно изменить спустя указанное количество часов после его предыдущего изменения.

Рекомендация: Задайте параметр равным *SYSVAL, если не наблюдается необычная активность смены пароля пользователем. В этом случае укажите другое значение, чтобы ограничить изменения пароля пользователем.

Локальное управление паролем

Параметр Локальное управление паролем (LCLPWDMGT) указывает, применяется ли локальное управление паролем пользовательского профайла. Если пароль не управляется локально, то пользователи могут входить в систему не напрямую, а только через другие платформы.

Если пароль управляется локально, то он хранится вместе с пользовательским профайлом. Это стандартный метод хранения пароля.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

LCLPWDMGT

Длина:

10

Если пароль не управляется локально, то для локального пароля i5/OS указывается значение *NONE. Пароль, указанный в параметре пароля, отправляется другим продуктам IBM, выполняющим синхронизацию паролей, таким как IBM i5/OS Integration for Windows Server. При этом пользователь не сможет изменить пароль с помощью команды Изменить пароль (CHGPWD). Кроме того, он не сможет напрямую войти в систему. Это значение влияет на другие продукты IBM, выполняющие синхронизацию паролей, такие как IBM i5/OS Integration for Windows Server.

Значение *NO рекомендуется указывать в этом параметре только в том случае, если пользователю требуется войти в систему с помощью другой платформы, такой как Windows Server.

Таблица 71. Возможные значения для параметра LCLPDMGT:

*YES	Локальное управление паролем.
*NO	Пароль не управляется локально.

Ограничить сеансы одним устройством

Поле Ограничить сеансы одним устройством указывает, ограничено ли число сеансов с устройствами для пользователя. Это значение не ограничивает меню Системный запрос и не запрещает второй вход в систему с одного и того же устройства.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

LMTDEVSSN

Длина:

7

Таблица 72. Возможные значения для параметра LMTDEVSSN:

*SYSVAL	Применяется системное значение QLMTDEVSSN.
*NO	Пользователь может одновременно войти в систему с помощью нескольких устройств.
*YES	Пользователь не может одновременно войти в систему с помощью нескольких устройств.
0	Для пользователя нет ограничений на число сеансов с устройствами. Это значение аналогично *NO.
1	Пользователю разрешен один сеанс с устройством. Это значение аналогично *YES.
2 - 9	Пользователю разрешено указанное число сеансов с устройствами.

Рекомендации: Запрет одновременного входа в систему с нескольких рабочих станций позволяет избежать совместное использование пользовательских профайлов. Рекомендуемое значение для системного значения QLMTDEVSSN - 1 (YES). Если пользователям необходимо одновременно входить в систему с нескольких рабочих станций, воспользуйтесь полем Ограничить сеансы одним устройством соответствующих пользовательских профайлов.

Буферизация нажатий клавиш

Этот параметр позволяет указать значение для буферизации клавиатуры, применяемое при инициализации задания для этого пользовательского профайла. Новое значение вступает в силу при следующем входе в систему.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

KBDBUF

Длина:

10

Поле буферизация клавиатуры управляет следующими функциями:

Буферизация ввода:

Пользователь может вводить данные быстрее, чем они отправляются системе.

Буферизация клавиши Attention:

Буферизация клавиши Attention позволяет обрабатывать клавишу Attention, также как и другие клавиши. При этом нажатие клавиши Attention приведет к отправке информации системе даже в том случае, если запрещен ввод с другой рабочей станции.

Таблица 73. Возможные значения для параметра KBDBUF:

*SYSVAL	Применяется системное значение QKBDBUF.
*NO	Функции буферизации ввода и клавиши Attention не применяются для этого пользовательского профайла.
*TYPEAHEAD	Для пользовательского профайла применяется функция буферизации ввода.
*YES	Для этого пользовательского профайла применяются функции буферизации ввода и клавиши Attention.

Максимальный объем памяти

Можно указать максимальный объем вспомогательной памяти, применяемой для хранения постоянных объектов, принадлежащих пользовательскому профайлу, включая объекты, помещенные в ходе выполнения задания во временную библиотеку (QTEMP).

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

MAXSTG

Длина:

11,0

Если для создания объекта требуется объем памяти, превышающий указанный максимальный объем, то такой объект не создается.

Максимальный объем памяти применяется независимо для всех пулов дисков (ASP) системы. Поэтому, значение 5000 указывает на то, что для пользовательского профайла доступна следующая вспомогательная память:

- 5000 Кб вспомогательной памяти из системного ASP и базовых ASP пользователей.
- 5000 Кб вспомогательной памяти из независимого ASP 00033 (если он существует).
- 5000 Кб вспомогательной памяти из независимого ASP 00034 (если он существует).

Это позволяет выделить 15000 Кб вспомогательной памяти всей системы.

При планировании максимального объема памяти для пользовательских профайлов учтите следующие системные функции, которые могут влиять на максимальный объем памяти, необходимый пользователю:

- Операция восстановления сначала присваивает память пользователю, а затем передает объект владельцу OWNER. В пользовательских профайлах, применяющихся для выполнения больших объемов операций восстановления, следует указать параметр MAXSTG(*NOMAX).
- Пользовательскому профайлу, которому принадлежит получатель журнала, память присваивается по мере увеличения размера получателя. В случае создания новых получателей пользовательскому профайлу, владеющему активным получателем журнала, присваивается новая память. В пользовательских профайлах, владеющих активными получателями журнала, следует указать параметр MAXSTG(*NOMAX).

- Если в пользовательском профайле указан параметр OWNER(*GRPPRF), то принадлежность всех объектов, созданных этим пользователем, передается профайлу группы. Однако для создания объекта пользователю потребуется достаточный объем памяти, так как перед передачей принадлежности группе этот объект сохраняется в этой памяти.
- Владельцу библиотеки память присваивается в соответствии с описаниями объектов, расположенных в этой библиотеке, даже в том случае, если они принадлежат другим пользователям. Примерами таких описаний могут служить ссылки на текст и программы.
- Пользовательским профайлам присваивается память для хранения временных объектов, применяемых в процессе обработки задания. Примерами таких объектов могут служить блоки управления фиксацией, области редактирования файлов и документы.

Таблица 74. Возможные значения для параметра MAXSTG:

*NOMAX	Пользовательскому профайлу присваивается любой запрашиваемый объем памяти.
<i>макс- Кб</i>	Укажите максимальный объем памяти в килобайтах (1 килобайт равен 1024 байтам), доступный для пользовательского профайла.

Ограничение приоритета

Параметр пользовательского профайла Ограничение приоритета определяет максимальные приоритеты планирования (приоритет задания и приоритет вывода) для заданий, отправляемых на выполнение. Ограничение приоритета управляет приоритетом представляемого задания. Также оно управляет изменениями приоритета задания, ожидающего в очереди, или выполняющегося задания.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

PTYLMT

Длина:

1

Для пакетного задания предусмотрено три различных значения приоритета:

Приоритет запуска:

Определяет приоритет выполняемого задания на использование системных ресурсов. Приоритет запуска задается в соответствии с классом задания.

Приоритет задания:

Определяет приоритет планирования для пакетного задания, расположенного в очереди заданий. Приоритет задания можно задать в описании задания или с помощью команды отправки.

Приоритет вывода:

Определяет приоритет планирования для вывода, созданного заданием, расположенным в очереди вывода. Приоритет вывода можно задать в описании задания или с помощью команды отправки.

Кроме того, параметр Ограничение приоритета позволяет ограничить изменения, которые пользователь, обладающий специальными правами доступа *JOBCTL, может внести в задания других пользователей. Заданию другого пользователя нельзя присвоить приоритет, превышающий ограничение, указанное в текущем пользовательском профайле.

Если пакетное задание выполняется от имени пользовательского профайла, не принадлежащего пользователю, передавшему задание на выполнение, то ограничения приоритета пакетного задания определяются пользовательским профайлом, от имени которого выполняется задание. Если запрашиваемый приоритет планирования задания, переданного на выполнение, превышает ограничение, указанное в пользовательском профайле, то приоритет задания уменьшается до значения, разрешенного пользовательским профайлом.

Таблица 75. Возможные значения для параметра PTYLMT:

3	По умолчанию для пользовательских профайлов ограничение приоритета равно 3. Приоритет задания и вывода по умолчанию равен 5. Ограничение приоритета в пользовательских профайлах значением 3 позволяет пользователям перемещать некоторые задания в очередях вперед других заданий.
<i>ограничение- приоритета</i>	Укажите значение от 1 до 9. Значение 1 соответствует максимальному приоритету, 9 - минимальному.

Рекомендации: Применение значений приоритетов в описаниях заданий и в командах передачи заданий на выполнение часто более предпочтительно для управления системными ресурсами, чем изменение ограничения приоритета в пользовательских профайлах.

Параметр Ограничение приоритета рекомендуется применять для управления изменениями, которые пользователь может вносить в задания, передаваемые на выполнение. Например, более высокий приоритет может потребоваться системным операторам для перемещения заданий в очередях.

Описание задания

Описание задания содержит набор атрибутов, связанных с заданием, таких как применяемая очередь заданий, приоритет планирования, данные выполнения, серьезность очереди сообщений, список библиотек и информация о выводе. Задание выполняется в системе в соответствии с этими атрибутами.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

JOB

Длина 10 (имя описания задания), 10 (имя библиотеки)

Права доступа:

*USE для описания задания, *READ и *EXECUTE для библиотеки

При входе пользователя в систему с помощью записи рабочей станции из описания подсистемы определяется описание задания, применяемое для интерактивного задания. Если в записи рабочей станции для описания задания указано значение *USRPRF, то применяется описание задания, заданное в пользовательском профайле.

Описание пакетного задания задается при запуске этого задания. Его можно указать по имени, либо применить описание задания из пользовательского профайла.

Дополнительная информация об описаниях заданий и работе с ними приведена в разделе Управление заданиями.

Таблица 76. Возможные значения для параметра JOB:

QDFTJOB	Применяется системное описание задания, расположенное в библиотеке QGPL. Для просмотра атрибутов, указанных в этом описании задания, воспользуйтесь командой Показать описание задания (DSPJOB).
<i>задание- описание- имя</i>	Укажите имя описания задания. Его длина не должна превышать 10 символов.

Таблица 77. Возможные значения для библиотеки JOB:

*LIBL	Для поиска описания задания применяется список библиотек.
*CURLIB	Описание задания выбирается с помощью текущей библиотеки задания. Если текущая библиотека не существует в списке библиотек, применяется QGPL.

Таблица 77. Возможные значения для библиотеки JOBD: (продолжение)

имя- библиотеки	Укажите библиотеку, в которой расположено описание задания. Длина имени не может превышать 10 символов.
-----------------	---

Рекомендации: Описание задания рекомендуется применять для управления доступом к библиотекам для интерактивных заданий. С помощью описания задания можно указать уникальный список библиотек для отдельного задания вместо применения системного значения QUSRLIBL (список пользовательских библиотек).

Профайл группы

Параметр Профайл группы (GRPPRF) указывает, является ли пользователь участником профайла группы. Пользователь, входящий в состав профайла группы, получает дополнительные права доступа к объектам. С помощью параметра Профайл дополнительной группы можно указать до 15 дополнительных групп.

Приглашение Добавить пользователя:

Группа пользователей

Параметр CL:

GRPPRF

Длина:

10

Права доступа:

Для того чтобы указать группу при создании или изменении пользовательского профайла, необходимы права доступа *OBJMGT, *OBJOPR, *READ, *ADD, *UPD и *DLT к соответствующему профайлу группы.

Прим.: Принятые права доступа не используются для проверки прав доступа *OBJMGT к профайлу группы. Дополнительная информация о принятых правах доступа приведена в разделе “Объекты, принимающие права доступа владельца” на стр. 156.

Если профайл группы указан в пользовательском профайле, то пользователю автоматически предоставляются права доступа *OBJMGT, *OBJOPR, *READ, *ADD, *UPD и *DLT. Эти права доступа необходимы для функций системы и их не следует удалять.

Если профайл, указанный в параметре GRPPRF, не является профайлом группы, система задает информацию в профайле, отмечая ее в качестве профайла группы. Кроме того, для профайла группы создается идентификатор группы (GID), если он не был указан.

Изменение значения GRPPRF вступает в силу при следующем входе пользователя в систему или при следующем переключении задания на пользовательский профайл, выполненном с помощью указателя профайла или маркера профайла, полученного после того, как произошло изменение.

Дополнительная информация о работе с профайлами групп приведена в разделе “Планирование профайлов групп” на стр. 251.

Таблица 78. Возможные значения для параметра GRPPRF:

*NONE	Профайл группы для этого пользовательского профайла не указан.
пользовательский-профайл	Укажите имя профайла группы, которому принадлежит этот пользователь.

Владелец

Если пользователь входит в состав группы, параметр пользовательского профайла Владелец позволяет указать владельца новых объектов, созданных пользователем. Объекты могут принадлежать как

пользователю, так и первой группе пользователя (значение параметра GRPPRF). Поле Владелец можно задать только в том случае, если задано значение, отличное от *NONE, в поле Профайл группы.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

OWNER

Длина:

10

- | Изменение значения Владелец вступает в силу при следующем входе пользователя в систему или при
- | следующем переключении задания на пользовательский профайл, выполненном с помощью указателя
- | профайла или маркера профайла, полученного после того, как произошло изменение.

Таблица 79. Возможные значения для параметра Owner:

*USRPRF	Владельцем всех создаваемых объектов является данный пользовательский профайл.
*GRPPRF	Владельцем всех объектов, создаваемых пользователем, является профайл группы. Этим объектам присваиваются права доступа *ALL. Пользовательскому профайлу особые права доступа к этим объектам не предоставляются. Если указано значение *GRPPRF, в параметре GRPPRF следует имя профайла группы, а в параметре GRPAUT - значение *NONE. Notes: 1. Все пользователи, входящие в состав группы, могут изменять, заменять и удалять объекты, принадлежащие этой группе. 2. Параметр *GRPPRF игнорируется всеми файловыми системами, кроме QSYS.LIB. В таких случаях по умолчанию владельцем объектов является пользователь.

Права доступа группы

Если пользовательский профайл входит в состав группы и указан параметр OWNER(*USRPRF), то поле Права доступа группы позволяет управлять правами доступа к объектам, созданным этим пользователем, которые получает профайл группы.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

GRPAUT

Длина:

10

Права доступа группы можно указать только в том случае, если в параметре OWNER указано значение *USRPRF, а в параметре GRPPRF - значение, отличное от *NONE. Права доступа группы применимы к профайлу, указанному в параметре GRPPRF. Они не применимы к профайлам дополнительных групп, указанным в параметре SUPGRPPRF.

- | Изменение значения GRPAUT вступает в силу при следующем входе пользователя в систему или при
- | следующем переключении задания на пользовательский профайл, выполненном с помощью указателя
- | профайла или маркера профайла, полученного после того, как произошло изменение.

Таблица 80. Возможные значения для параметра GRPAUT:

*NONE	Особые права доступа к объектам, создаваемым пользователем, профайлу группы не предоставляются.
--------------	---

Таблица 80. Возможные значения для параметра GRPAUT: (продолжение)

*ALL	Профайлу группы предоставляются полные права доступа к новым объектам, созданным пользователем.
*CHANGE	Профайлу группы предоставляются права доступа на изменение новых объектов, созданных пользователем.
*USE	Профайлу группы предоставляются права доступа на просмотр новых объектов, созданных пользователем.
*EXCLUDE	Профайлу группы запрещено предоставлять права доступа к новым объектам, созданным пользователем.

Ссылки, связанные с данной

“Определение режима доступа к информации” на стр. 138

Можно указать, какие операции разрешены с объектами, данными и полями.

Тип прав доступа группы

Параметр пользовательского профайла Тип прав доступа группы определяет тип прав доступа к новым объектам создаваемым пользователем, которые предоставляются группе пользователя.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

GRPAUTTYR

Длина:

10

Параметр GRPAUTTYR совместно с параметрами OWNER, GRPPRF и GRPAUT позволяет определить права доступа группы к новым объектам.

- | Изменение значения GRPAUTTYR вступает в силу при следующем входе пользователя в систему или при
- | следующем переключении задания на пользовательский профайл, выполненном с помощью указателя
- | профайла или маркера профайла, полученного после того, как произошло изменение.

Таблица 81. Возможные значения для параметра GRPAUTTYR: ¹

*PRIVATE	Права доступа, определенные с помощью параметра GRPAUT, присваиваются профайлу группы в качестве частных прав доступа.
*PGP	Профайл группы, определенный с помощью параметра GRPPRF, является основной группой для новых объектов. Права доступа основной группы указаны в параметре GRPAUT. Это значение можно указывать, только если GRPAUT не равно *NONE.
¹	Частные права доступа и права доступа основной группы обеспечивают одинаковый доступ к объекту для членов группы, но могут отличаться по производительности. На рисунке “Основная группа объекта” на стр. 151 показан принцип действия прав доступа основной группы.

Рекомендации: Для того чтобы начать использовать права доступа основной группы, укажите значение *PGP. Для пользователей, создающих много новых объектов, которые должны быть доступны членам профайла группы, рекомендуется указывать параметр GRPAUTTYR(*PGP).

Дополнительные группы

Дополнительные группы можно указать при создании или изменении пользовательского профайла. Если в параметре GRPPRF указано значение *NONE, то пользователь не может входить в состав дополнительных групп.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

SUPGRPPRF

Длина:

150

Права доступа:

Для того чтобы указать дополнительные группы при создании или изменении пользовательского профайла, необходимы права доступа *OBJMGT, *OBJOPR, *READ, *ADD, *UPD и *DLT к соответствующему профайлу группы.

Прим.: В данном случае недопустимо применение принятых прав доступа *OBJMGT. Более подробная информация приведена в разделе “Объекты, принимающие права доступа владельца” на стр. 156.

Можно указать до 15 имен профайлов, права доступа которых будут предоставлены пользователю. Пользователь становится членом всех дополнительных групп.

Если профайлы дополнительных групп указаны в пользовательском профайле, то пользователю автоматически предоставляются права доступа *OBJMGT, *OBJOPR, *READ, *ADD, *UPD и *DLT. Эти права доступа необходимы для функций системы и их не следует удалять. Если профайл, указанный в параметре SUPGRPPRF не является профайлом группы, система отмечает его в качестве профайла группы. Кроме того, для профайла группы создается идентификатор группы (GID), если он не был указан.

Изменение значения SUPGRPPRF вступает в силу при следующем входе пользователя в систему или при следующем переключении задания на пользовательский профайл, выполненном с помощью указателя профайла или маркера профайла, полученного после того, как произошло изменение.

Дополнительная информация о работе с профайлами групп приведена в разделе “Планирование профайлов групп” на стр. 251.

Таблица 82. Возможные значения для параметра SUPGRPPRF:

*NONE	Дополнительные группы для этого пользовательского профайла не указаны.
<i>имя- профайла- группы</i>	Укажите до 15 имен профайлов групп для применения в этом пользовательском профайле. Пользователю предоставляются права доступа этих профайлов, а также профайлов, указанных в параметре GRPPRF. В качестве одного из 15 дополнительных профайлов групп можно также указать имя профайла, заданное в параметре GRPPRF.

Код учета ресурсов

Код учета ресурсов позволяет собрать информацию об использовании системных ресурсов заданием.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

ACGCDE

Длина:

15

Учет ресурсов задания представляет собой дополнительную функцию, позволяющую собирать информацию об использовании системных ресурсов. Системное значение уровень учета ресурсов (QACGLVL) позволяет включить или выключить функцию учета ресурсов. Код учета ресурсов для задания указан либо в описании задания, либо пользовательском профайле. Кроме того, код учета ресурсов можно указать с помощью команды Изменить код учета ресурсов (CHGACGCDE) во время выполнения задания.

- | Изменение значения *кода учета ресурсов* вступает в силу при следующем входе пользователя в систему или
- | при следующем запуске задания с кодом учета ресурсов пользовательского профайла.

Дополнительная информация об учете ресурсов задания приведена в разделе Управление заданиями.

Таблица 83. Возможные значения для параметра *ACGCDE*:

*BLANK	Этому пользовательскому профайлу присваивается код учета ресурсов, состоящий из 15 пробелов.
<i>код-учета-ресурсов</i>	Укажите код учета ресурсов. Длина кода ресурсов не может превышать 15 символов. Если указано меньше 15 символов, то в эту строку справа добавляется необходимое число пробелов.

Пароль документов

Для пользователя можно указать пароль документа, позволяющий защитить личные электронные письма пользователя от просмотра сотрудниками, работающими от его имени. Пароль документа поддерживается многими продуктами Архитектуры обмена документами (DIA), такими как Displaywriter.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

DOCPWD

Таблица 84. Возможные значения для параметра *DOCPWD*:

*NONE	Пароль документа не задается.
<i>пароль- документа</i>	Укажите пароль документа для этого пользователя. Длина пароля должна лежать в диапазоне от 1 до 8 символов (допустимы буквы от A до Z и цифры от 0 до 9). Первый символ пароля должен быть алфавитным, остальные могут быть цифрами. Запрещены внутренние и начальные пробелы, а также специальные символы.

Очередь сообщений

Очередь сообщений представляет собой объект, в который заносятся сообщения, отправляемые пользователю или программе. Очередь сообщений применяется, если пользователь отправляет или получает сообщения.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

MSGQ

Длина:

10 (имя очереди сообщений), 10 (имя библиотеки)

Права доступа:

*USE для очереди сообщений, если она существует. *EXECUTE для библиотеки очереди сообщений.

Если очередь сообщений не существует, она создается в случае создания или изменения профайла. Очередь сообщений принадлежит создаваемому или изменяемому профайлу. Пользователю, создавшему профайл, предоставляются права доступа *ALL к этой очереди сообщений.

Если очередь сообщений пользовательского профайла изменяется с помощью команды Изменить пользовательский профайл (CHGUSRPRF), предыдущая очередь сообщений не удаляется.

Таблица 85. Возможные значения для параметра MSGQ:

*USRPRF	В качестве очереди сообщений применяется очередь сообщений, имя которой совпадает с именем пользовательского профайла. Если очередь сообщений не существует, она создается в библиотеке QUSRSYS.
<i>очередь- сообщений</i>	Укажите имя очереди сообщений для пользователя. Кроме имени очереди сообщений необходимо указать параметр библиотеки.

Таблица 86. Возможные значения для библиотеки MSGQ:

*LIBL	Для выбора очереди сообщений применяется список библиотек. Если очередь сообщений не существует, значение *LIBL указать нельзя.
*CURLIB	Для выбора очереди сообщений применяется текущая библиотека. Если текущая библиотека не существует в списке библиотек, применяется QGPL. Если очередь сообщений не существует, она создается в текущей библиотеке или библиотеке QGPL.
<i>имя- библиотеки</i>	Укажите имя библиотеки, в которой расположена очередь сообщений. Если очередь сообщений не существует, она создается в этой библиотеке.

Рекомендации: Указывайте для каждого пользовательского профайла уникальную очередь сообщений, предпочтительно с таким же именем.

Доставка

Режим доставки в очередь сообщений определяет, следует ли прерывать работу пользователя в случае поступления в очередь новых сообщений.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

DLVRY

Длина:

10

Режим доставки, указанный в пользовательском профайле, применим только к частной очереди сообщений пользователя. Изменения, внесенные в режим доставки в очередь сообщений, указанный в пользовательском профайле, применяются при следующем входе в систему. Кроме того, режим доставки в очередь сообщений можно изменить с помощью команды Изменить очередь сообщений (CHGMSGQ).

Таблица 87. Возможные значения для параметра DLVRY:

*NOTIFY	Уведомление о поступлении нового сообщения отправляется заданию, которому присвоена очередь сообщений. Для интерактивных заданий на рабочих станциях подается звуковой сигнал и загорается индикатор ожидающего сообщения. Если очередь сообщений используется совместно с другими пользователями, то тип доставки нельзя изменить на *NOTIFY.
*BREAK	В случае поступления нового сообщения задание, которому присвоена очередь сообщений, прерывается. Для интерактивного задания подается звуковой сигнал (если установлено необходимое аппаратное обеспечение). Если очередь сообщений используется совместно с другими пользователями, то тип доставки нельзя изменить на *BREAK.
*HOLD	Сообщения блокируются в очереди сообщений до тех пор, пока пользователь их не запросит.
*DFT	Для сообщений, ответ на которые обязателен, отправляется ответ по умолчанию. Информационные сообщения игнорируются.

Серьезность

Если очередь сообщений работает в режиме *BREAK или *NOTIFY, код серьезности определяет минимальный уровень сообщений, доставляемых пользователю. Сообщения, уровень которых ниже минимального, блокируются в очереди сообщений без уведомления пользователей.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

SEV

Длина:

2,0

Изменения, внесенные в серьезность очереди сообщений, указанную в пользовательском профайле, применяются при следующем входе в систему. Кроме того, серьезность очереди сообщений можно изменить с помощью команды Изменить очередь сообщений (CHGMSGQ).

Таблица 88. Возможные значения для параметра SEV:

00:	Если код серьезности не указан, применяется 00. В режиме *NOTIFY или *BREAK пользователь получает уведомления о всех поступающих сообщениях.
<i>код-серьезности</i>	Укажите значение от 00 до 99, определяющее минимальный код серьезности для уведомления. Допустимы любые двузначные значения, даже если код серьезности для них не определен системой или пользователем.

Принтер

Можно указать принтер для печати вывода пользователя. Если в качестве принтера (*DEV) указана очередь вывода (OUTQ), то имена буферных файлов, помещаемых в очередь вывода, совпадают с именем принтера.

Приглашение Добавить пользователя:

Принтер по умолчанию

Параметр CL:

PRTDEV

Длина:

10

Информация о принтере и очереди вывода, указанная в пользовательском профайле, применяется если для файла принтера задано значение *JOB, а в описании задания - значение *USRPRF. Дополнительная информация о направлении вывода на принтер приведена в разделе Основы печати.

Таблица 89. Возможные значения для параметра PRTDEV:

*WRKSTN	Применяется принтер, присвоенный рабочей станции пользователя в описании устройства.
*SYSVAL	Применяется принтер системы по умолчанию, указанный с помощью системного значения QPRTDEV.
<i>название-устройства-принтера</i>	Укажите имя принтера для печати вывода пользователя.

Очереди вывода

В результате как интерактивной, так и пакетной обработки могут создаваться буферные файлы, отправляемые на печать. Буферные файлы заносятся в очередь вывода. В системе могут существовать несколько очередей вывода.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:
OUTQ

Длина:
10 (имя очереди вывода), 10 (имя библиотеки)

Права доступа:
*USE для очереди вывода, *EXECUTE для библиотеки

Очередь вывода не обязательно должна быть связана с принтером для получения новых буферных файлов.

Информация о принтере и очереди вывода, указанная в пользовательском профайле, применяется если для файла принтера задано значение *JOB, а в описании задания - значение *USRPRF. Дополнительная информация о печати вывода на принтер приведена в разделе Расширенная презентация функций.

Таблица 90. Возможные значения для параметра OUTQ:

*WRKSTN	Применяется очередь вывода, присвоенная рабочей станции пользователя, в описании устройства.
*DEV	Применяется очередь вывода, имя которой совпадает с именем принтера, указанного в параметре PRTDEV.
<i>имя- очереди- вывода</i>	Укажите имя очереди вывода. Очередь вывода должна уже существовать. Кроме очереди вывода, необходимо указать библиотеку.

Таблица 91. Возможные значения для библиотеки OUTQ:

*LIBL	Для выбора очереди вывода применяется список библиотек.
*CURLIB	Для выбора очереди вывода применяется текущая библиотека. Если текущая библиотека не существует в списке библиотек, применяется QGPL.
<i>имя- библиотеки</i>	Укажите имя библиотеки, в которой расположена очередь вывода.

Программа обработки клавиши Attention

Программа обработки клавиши Attention (ATNPGM) представляет собой программу, вызываемую при нажатии клавиши Attention (ATTN) в интерактивном задании.

Приглашение Добавить пользователя:
Не показывается

Параметр CL:
ATNPGM

Длина:
10 (имя программы) 10 (имя библиотеки)

Права доступа:
*USE для программы
*EXECUTE для библиотеки

ATNPGM можно активировать только в том случае, если в качестве программы выполнения указана QCMD. Активация ATNPGM выполняется до вызова начальной программы. Если начальная программа изменяет ATNPGM, то новая ATNPGM активируется только на время выполнения начальной программы. Если выполнить команду Выбрать программу обработки клавиши Attention (SETATNPGM) из командной строки или приложения, то новая ATNPGM переопределяет ATNPGM, указанную в пользовательском профайле.

Примечание: Дополнительная информация о последовательности обработки при входе в систему приведена в разделе “Запуск интерактивного задания” на стр. 209.

Поле *Ограничить возможности* позволяет разрешить или запретить изменение программы обработки клавиши Attention с помощью команды Изменить пользовательский профайл (CHGPRF).

Таблица 92. Возможные значения для параметра ATNPGM:

*SYSVAL	Применяется системное значение QATNPGM.
*NONE	Программа обработки клавиши Attention не применяется.
*ASSIST	Применяется Программа Attention операционной поддержки (QEZMAIN).
<i>имя- программы</i>	Укажите имя программы обработки клавиши Attention. Кроме имени программы необходимо указать библиотеку.

Таблица 93. Возможные значения для библиотеки ATNPGM:

*LIBL	Для поиска программы обработки клавиши Attention применяется список библиотек.
*CURLIB	Для выбора программы обработки клавиши Attention применяется текущая библиотека. Если текущая библиотека не существует в списке библиотек, применяется QGPL.
<i>имя- библиотеки</i>	Укажите имя библиотеки, в которой расположена программа обработки клавиши Attention.

Последовательность сортировки

Последовательность применяется для вывода этого пользователя. Для этого можно применять системные таблицы или создать собственные. Таблица сортировки может быть связана с конкретным идентификатором языка системы.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

SRTSEQ

Длина:

10 (значение или имя таблицы), 10 (имя библиотеки)

Права доступа:

*USE для таблицы, *EXECUTE для библиотеки

Таблица 94. Возможные значения для параметра SRTSEQ:

*SYSVAL	Применяется системное значение QSRTSEQ.
*HEX	Применяется стандартная шестнадцатеричная последовательность сортировки.
*LANGIDSHR	Применяется таблица последовательности сортировки, связанная с идентификатором языка. Для различных символов может быть указано один и тот же вес.
*LANGIDUNQ	Применяется таблица последовательности сортировки, связанная с идентификатором языка. Для каждого символа кодовой страницы должен быть указан уникальный вес.
<i>имя-таблицы</i>	Укажите имя таблицы последовательности сортировки.

Таблица 95. Возможные значения для библиотеки SRTSEQ:

*LIBL	Для поиска таблицы, указанной для значения SRTSEQ, применяется список библиотек.
--------------	--

Таблица 95. Возможные значения для библиотеки SRTSEQ: (продолжение)

*CURLIB	Для поиска таблицы, указанной для значения SRTSEQ, применяется текущая библиотека. Если текущая библиотека не существует в списке библиотек, применяется QGPL.
<i>имя- библиотеки</i>	Укажите имя библиотеки, в которой расположена таблица последовательности сортировки.

Идентификатор языка

Для пользователя можно указать идентификатор языка.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

LANGID

Длина:

10

Для того чтобы просмотреть список идентификаторов языков в меню Создать пользовательский профайл или Изменить пользовательский профайл нажмите клавишу F4 (приглашение) для параметра идентификатора языка.

Таблица 96. Возможные значения для параметра LANGID:

*SYSVAL:	Для определения идентификатора языка применяется системное значение CoD.
<i>идентификатор- языка</i>	Укажите идентификатор языка для пользователя.

Идентификатор страны или региона

Можно указать идентификатор страны или региона, применяемый системой для пользователя.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

CNTRYID

Длина:

10

Для того чтобы просмотреть список идентификаторов стран и регионов в меню Создать пользовательский профайл или Изменить пользовательский профайл нажмите клавишу F4 (приглашение) для параметра идентификатора страны или региона.

Таблица 97. Возможные значения для CNTRYID:

*SYSVAL	Для определения идентификатора страны или региона применяется системное значение QCNTRYID.
<i>идентификатор-страны-или- региона</i>	Укажите идентификатор страны или региона для пользователя.

Идентификатор набора символов

Можно указать идентификатор набора символов, применяемый системой для пользователя.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:
CCSID

Длина:
5,0

Для того чтобы просмотреть список идентификаторов наборов символов в меню Создать пользовательский профайл или Изменить пользовательский профайл нажмите клавишу F4 (приглашение) для параметра идентификатора набора символов.

Таблица 98. Возможные значения для параметра CCSID:

*SYSVAL	Для определения идентификатора набора символов применяется системное значение QCCSID.
<i>идентификатор-набора- символов</i>	Укажите идентификатор набора символов для пользователя.

Управляющий элемент символьного идентификатора

Атрибут *CHRIDCTL* позволяет управлять типом преобразования набора символов, выполняемого для файлов дисплея, файлов принтера и групп панелей.

Приглашение Добавить пользователя:
Не показывается

Параметр CL:
CHRIDCTL

Длина:
10

Информация управления идентификаторами символов, указанная в пользовательских профайлах, применяется только в том случае, если в параметре CHRID команд создания, изменения и переопределения файлов дисплея, файлов принтера и групп панелей задано специальное значение *CHRIDCTL.

Таблица 99. Возможные значения для параметра CHRIDCTL:

*SYSVAL	Управление идентификатором символов определяется с помощью системного значения QCHRIDCTL.
*DEV D	Для представления CCSID данных применяется CHRID устройства. Преобразование не выполняется, так как CCSID данных всегда совпадает с CHRID устройства.
*JOBCCSID	Преобразование символов выполняется, если отличаются значения CHRID устройства, CCSID задания, CCSID данных. Вводимые символьные данные при необходимости преобразуются из CHRID устройства в CCSID задания. Выводимые символьные данные при необходимости преобразуются из CCSID задания в CHRID устройства. Выводимые символьные данные при необходимости преобразуются из CCSID файла или группы панелей в CHRID устройства.

Атрибуты задания

Поле SETJOBATR задает атрибуты задания, загружаемые при инициализации задания из локали, указанной с помощью параметра LOCALE.

Приглашение Добавить пользователя:
Не показывается

Параметр CL:
SETJOBATR

Длина:
160

Таблица 100. Возможные значения для параметра SETJOBATR:

*SYSVAL	Для определения атрибутов, загружаемых из локали применяется системное значение QSETJOBATR.
*NONE	Атрибуты из локали не загружаются.
*CCSID	Применяется идентификатор набора символов (CCSID) локали. Значение CCSID локали переопределяет CCSID, указанный в пользовательском профайле.
*DATFMT	Применяется формат даты локали.
*DATSEP	Применяется разделитель даты локали.
*DECfmt	Применяется десятичный формат локали.
*SRTSEQ	Применяется последовательность сортировки локали. Последовательность сортировки локали переопределяет последовательность сортировки, указанную в пользовательском профайле.
*TIMSEP	Применяется разделитель времени локали.

Допустима любая комбинация следующих значений:

- *CCSID
- *DATFMT
- *DATSEP
- *DECfmt
- *SRTSEQ
- *TIMSEP

Локаль

Поле Локаль задает путь к локали, присвоенной этому пользователю в переменной среды LANG.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

LOCALE

Таблица 101. Возможные значения для параметра LOCALE:

*SYSVAL	Для определения пути к локали для этого пользователя применяется системное значение QLOCALE.
*NONE	Локаль пользователю не присваивается.
*C	Пользователю присваивается локаль C.
*POSIX	Пользователю присваивается локаль POSIX.
<i>путь-к-локали</i>	Путь к локали, которую необходимо присвоить этому пользователю.

Опции пользователя

Поле Опции пользователя позволяет настроить некоторые системные меню и функции, доступные пользователю. В параметре опции пользователя можно указать несколько значений.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

USROPT

Длина:

240 (по 10 символов)

Таблица 102. Возможные значения для параметра USROPT:

*NONE	Для пользователя специальные опции не применяются. Применяется стандартный системный интерфейс.
*CLKWD	В приглашении ввода команды CL вместо возможных значений параметров отображаются ключевые слова. В обычном приглашении ввода команды CL для этого необходимо нажать клавишу F11.
*EXPERT	В меню, в которых показаны права доступа к объектам, таких как Редактировать права доступа к объекту или Редактировать список прав доступа, отображается подробная информация о правах доступа. Для этого не нужно нажимать клавишу F11 (Показать сведения). На рисунке “Меню прав доступа” на стр. 162 показана расширенная версия меню.
*HLPFULL	Вместо окна показывается полноэкранный справочник.
*PRTMSG	В очередь сообщений пользователя отправляется уведомление о печати буферного файла этого пользователя.
*ROLLKEY	Действия клавиш Page Up и Page Down инвертируются.
*NOSTMSG	Не отображаются сообщения о состоянии, которые обычно выводятся в нижней части экрана.
*STSMMSG	Сообщения о состоянии показываются пользователю.

Идентификатор пользователя

Для идентификации и проверки прав доступа пользователя в интегрированной файловой системе применяется номер ИД пользователя (UID). Для каждого пользователя системы должен быть задан уникальный номер ИД пользователя.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

UID

Длина:

10,0

Таблица 103. Возможные значения для параметра UID:

*GEN	Номер ИД пользователя создается системой. Значение UID будет превышать 100.
<i>uid</i>	Значение от 1 до 4294967294, присваиваемое пользователю в качестве UID. Это значение должно быть уникальным.

Рекомендации: Как правило рекомендуется задать параметр UID(*GEN) для того, чтобы номера ИД пользователя автоматически создавались системой. Однако, если система подключена к сети, то могут потребоваться UID, совпадающие с идентификаторами, заданными для пользователей в других системах. Обратитесь к администратору сети.

Номер ИД группы

Для идентификации профайла в качестве профайла группы в интегрированной файловой системе применяется номер ИД группы (GID). Для профайлов, применяемых в качестве профайлов групп, должен быть указан уникальный GID.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

GID

Длина:
10,0

Таблица 104. Возможные значения для параметра GID:

*NONE	Для профайла GID не задается. Это значение необходимо указать, если пользовательский профайл входит в группу (GRPPRF на равно *NONE).
*GEN	Номер ИД группы создается системой. Значение GID будет превышать 100.
<i>gid</i>	Значение от 1 до 4294967294, присваиваемое профайлу в качестве GID. Это значение должно быть уникальным.

Рекомендации: Как правило рекомендуется задать параметр GID(*GEN) для того, чтобы номера ИД групп автоматически создавались системой. Однако, если система подключена к сети, то могут потребоваться GID, совпадающие с идентификаторами, заданными для пользователей в других системах. Обратитесь к администратору сети.

Не рекомендуется присваивать GID пользовательскому профайлу, который вы не планируете применять в качестве профайла группы. В некоторых средах пользователю, для которого указан GID, запрещено выполнять различные функции.

Домашний каталог

Домашний каталог представляет собой начальный рабочий каталог пользователя в интегрированной файловой системе. Кроме того, если для пользователя не указан текущий каталог, то применяется домашний каталог.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

HOMEDIR

Если при входе в систему домашний каталог, указанный в профайле, не существует, то в качестве домашнего каталога применяется корневого каталог (/).

Таблица 105. Возможные значения для параметра HOMEDIR:

*USRPRF	Пользователю присваивается домашний каталог с именем /home/xxxxx, где xxxxx - имя пользовательского профайла.
<i>домашний-каталог</i>	Имя домашнего каталога, присваиваемого пользователю.

Связь EIM

Параметр Связь EIM указывает, будет ли добавлена в идентификатор EIM пользователя связь EIM (преобразование идентификаторов в рамках предприятия). Если идентификатор EIM не существует, его можно создать.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

EIMASSOC

Notes:

1. Информация о связи EIM не предназначена для хранения в пользовательском профайле. Она не сохраняется в пользовательском профайле и не восстанавливается из него.
2. Если система не настроена для работы с технологией EIM, то обработка не выполняется. Если команде не удастся выполнить операции EIM, то это не приводит к сбою.

Таблица 106. Возможные значения для параметра EIMASSOC, одиночные значения:

Одиночные значения	
*NOCHG	Связь EIM не добавляется.

Таблица 107. Возможные значения для параметра EIMASSOC, элемент 1:

Элемент 1: Идентификатор EIM	
Задает идентификатор EIM для связи.	
*USRPRF	Имя идентификатора EIM совпадает с именем пользовательского профайла.
<i>символьное-значение</i>	Задает имя идентификатора EIM.

Таблица 108. Возможные значения для параметра EIMASSOC, элемент 2:

Элемент 2: Тип связи	
Задает тип связи. Для пользователей i5/OS рекомендуется задавать целевые связи.	
Целевые связи используются для защиты существующих данных. Они возвращаются в результате операций поиска связанного идентификатора (например, <code>eimGetTargetFromSource()</code>) и не могут использоваться в качестве исходного пользовательского профайла операции поиска связанного идентификатора.	
Исходный связи как правило применяются для целей идентификации. Они применяются в качестве исходного пользовательского профайла операции поиска связанного идентификатора и не могут быть найдены в результате операций поиска связанного идентификатора.	
С помощью административных связей можно определить, что пользовательский профайл связан в идентификатором EIM. Их нельзя использовать в качестве исходных или целевых.	
*TARGET	Обработка целевой связи.
*SOURCE	Обработка исходной связи.
*TGTSRC	Обработка как целевой, так и исходной связи.
*ADMIN	Обработка административной связи.
*ALL	Обработка связей всех типов.

Таблица 109. Возможные значения для параметра EIMASSOC, элемент 3:

Элемент 3: Действие для связи	
*REPLACE	Связи указанного типа удаляются из всех идентификаторов EIM, связанных с этим пользовательским профайлом и локальным реестром EIM. В указанный идентификатор EIM будет добавлена новая связь.
*ADD	Добавить связь.
*REMOVE	Удалить связь.

Таблица 110. Возможные значения для параметра EIMASSOC, элемент 4:

Элемент 4: Создать идентификатор EIM	
Позволяет создать идентификатор EIM, если он не существует.	
*NOCRTEIMID	Идентификатор EIM не создается.
*CRTEIMID	Идентификатор EIM создается, если он не существует.

Права доступа

Поле Права доступа позволяет указать общие права доступа к пользовательскому профайлу.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

AUT

Права доступа к пользовательскому профайлу управляют различными функциями, связанными с профайлом:

- Изменение профайла
- Показ профайла
- Удаление профайла
- Передача задание на выполнение от имени профайла
- Указание профайла в описании задания
- Передача профайлу прав доступа к объекту
- Добавление элементов, если это профайл группы

Таблица 111. Возможные значения для параметра AUT:

*EXCLUDE	Общий доступ к пользовательскому профайлу запрещен.
*ALL	Предоставляются полные общие права доступа к пользовательскому профайлу.
*CHANGE	Общие права доступа к пользовательскому профайлу включают в себя только права на изменение.
*USE	Предоставляются общие права доступа на просмотр информации о пользовательском профайле.

Полное описание прав доступа, которые можно предоставить, приведено в разделе “Определение режима доступа к информации” на стр. 138.

Рекомендации: Для того чтобы предотвратить несанкционированное использование пользовательских профайлов, обладающих правами доступа к особо важным объектам, убедитесь, что для них указаны общие права доступа *EXCLUDE. С помощью профайлов можно передать задание на выполнение от имени этого профайла или изменить программу, в результате чего она сможет принимать права доступа этого профайла.

Контроль объекта

Значение контроля за объектом, указанное в пользовательском профайле, используется совместно со значением контроля за объектом, указанным для объекта, для определения необходимости контроля за пользователем, работающим с этим объектом.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

OBJAUD

Длина:

10

Контроль за объектом нельзя указать в пользовательских командах. Для того чтобы задать это значение для пользователя воспользуйтесь командой CHGUSRAUD. Команда CHGUSRAUD доступна только для пользователей, обладающих правами доступа *AUDIT.

Таблица 112. Возможные значения для параметра OBJAUD:

*NONE	Необходимость контроля за пользователем определяется в соответствии со значениями OBJAUD, указанными для объектов.
--------------	--

Таблица 112. Возможные значения для параметра OBJAUD: (продолжение)

*ALL	Если в параметре OBJAUD для объекта указано значение *USRPRF, то в случае изменения или чтения этого объекта пользователем заносится контрольная запись.
*CHANGE	Если в параметре OBJAUD для объекта указано значение *USRPRF, то в случае изменения этого объекта пользователем заносится контрольная запись.
*NOTAVL	Означает, что значение параметра недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение параметру нельзя.

В таблице Табл. 113 показано, каким образом значения OBJAUD, указанные для пользователей и объектов, используются вместе:

Таблица 113. Контроль за доступом к объекту

Значение OBJAUD для объекта	Значение OBJAUD для пользователя		
	*NONE	*CHANGE	*ALL
*ALL	Изменение и использование	Изменение и использование	Изменение и использование
*CHANGE	Изменение	Изменение	Изменение
*NONE	Нет	Нет	Нет
*USRPRF	Нет	Изменение	Изменение и использование

Задачи, связанные с данной

“Планирование контроля доступа к объектам” на стр. 304

Операционная система i5/OS предоставляет возможность сохранять в журнале контроля за действиями информацию о доступе к объекту. Для этого используются системные значения и значения контроля за за объектом для пользователей и объектов. Это называется *контролем за объектом*.

Контроль действий

Для каждого пользователя можно указать действия, связанные с защитой, которые следует регистрировать в журнале контроля за действиями. Действия, указанные для отдельных пользователей применяются совместно с действиями, указанными для всех пользователей с помощью системных значений QAUDLVL и QAUDLVL2.

Приглашение Добавить пользователя:

Не показывается

Параметр CL:

AUDLVL

Длина:

640

Контроль действий объектом нельзя указать с помощью пользовательских меню. Для этого предназначена команда CHGUSRAUD. Команда CHGUSRAUD доступна только для пользователей, обладающих правами доступа *AUDIT.

Таблица 114. Возможные значения для параметра AUDLVL:

*NONE	Контроль действий определяется в соответствии с системным значением QAUDLVL. Дополнительный контроль действий не выполняется.
*NOTAVL	Означает, что значение параметра недоступно для пользователя, поскольку у того нет ни специальных прав доступа *AUDIT, ни специальных прав доступа *ALLOBJ. Присвоить это значение параметру нельзя.

Таблица 114. Возможные значения для параметра AUDLVL: (продолжение)

	*AUTFAIL	Контролируются ошибки авторизации.
	*CMD	Регистрируются действия, связанные с командной строкой. Значение *CMD можно указать только для отдельных пользователей. Функция контроля командной строки недоступна в качестве опции уровня системы в системном значении QAUDLVL.
	*CREATE	Регистрируются операции, связанные с созданием объектов.
	*DELETE	Регистрируются операции, связанные с удалением объектов.
	*JOBBAS	Контролируются основные функции заданий.
	*JOBCHGUSR	Контролируются изменения профайла пользователя или группы активной нити.
	*JOBDTA¹	Регистрируются изменения заданий.
	*OBJMGT	Регистрируются операции по перемещению и переименованию объектов.
	*OFCSRVR	Регистрируются изменения, вносимые в системный каталог рассылки и действия, связанные с электронной почтой.
	*NETBAS	Контролируются основные сетевые функции.
	*NETCLU	Контролируются операции, связанные с кластером или группой ресурсов кластера.
	*NETCMN³	Контролируются функции сети и связи.
	*NETFAIL	Контролируются ошибки сети.
	*NETSCK	Контролируются задачи сокетов.
	*OPTICAL	Контролируются все оптические функции.
	*PGMADP	Регистрируются случаи получения прав доступа от программы, принимающей права доступа.
	*PGMFAIL	Контролируются ошибки программ.
	*PRTDTA	Контролируются функции с параметром SPOOL(*NO).
	*SAVRST	Регистрируются операции по сохранению и восстановлению объектов.
	*SECCFG	Контролируется конфигурация защиты.
	*SECDIRSRV	Контролируются изменения и обновления при выполнении функций службы каталогов.
	*SECIPC	Контролируются изменения, вносимые в обмен данными между процессами.
	*SECNAS	Контролируются действия службы сетевой идентификации.
	*SECRUN	Контролируются базовые функции защиты.
	*SECCKD	Контролируются дескрипторы сокетов.
	*SECURITY²	Регистрируются функции, связанные с защитой.
	*SECVFY	Контролируется работа с функциями проверки.
	*SECVLDL	Контролируются изменения, вносимые в объекты контрольных списков.
	*SERVICE	Контролируется работа со служебными средствами.
	*SPLFDTA	Регистрируются действия, выполняемые над буферными файлами.
	*SYSMGT	Регистрируется работа с функциями управления системами.

Таблица 114. Возможные значения для параметра AUDLVL: (продолжение)

1	<p>*JOBDDTA включает значения *JOBDBAS и *JOBCHGUSR, позволяющие точнее настроить контроль. Если указаны оба эти значения, то результат будет аналогичен тому, как если бы было указано только значение *JOBDDTA.</p>
2	<p>*SECURITY состоит из нескольких значений, позволяющих выполнить более точную настройку контроля. Если указаны все эти значения, то результат будет аналогичен тому, как если бы было указано только значение *SECURITY. Эти значения перечислены ниже.</p> <ul style="list-style-type: none">• *SECDFG• *SECDFSRV• *SECDFPC• *SECDFNAS• *SECDFRUN• *SECDFCKD• *SECDFVY• *SECDFVLDL
3	<p>Значение *NETCMN состоит из нескольких значений контроля, позволяющих более точно настроить функцию контроля. Если указаны все эти значения, то результат будет аналогичен тому, как если бы было указано только значение *NETCMN. Эти значения перечислены ниже.</p> <ul style="list-style-type: none">• *NETDBAS• *NETDFCLU• *NETDFFAIL• *NETDFSCK

Ссылки, связанные с данной

“Планирование контроля действий” на стр. 278

Для контроля действий используются системные значения QAUDCTL (управление контролем), QAUDLVL (уровень контроля), QAUDLVL2 (расширение уровня контроля), а также параметр AUDLVL (контроль действий) из пользовательских профайлов.

Дополнительная информация, связанная с пользовательскими профайлами

В этом разделе обсуждаются частные права доступа, информация о принадлежности объекта и информация об объекте главной группы, относящиеся к пользовательскому профайлу.

Ссылки, связанные с данной

“Хранение информации о защите” на стр. 260

Для правильного планирования процедур резервного копирования и восстановления необходимо хорошо понимать принципы сохранения и восстановления информации.

Частные права доступа

Все частные права доступа к объектам хранятся в пользовательских профайлах. Если пользователю требуется доступ к объекту, соответствующие права доступа можно найти в частных правах доступа пользователя.

Более подробная информация о проверке прав доступа приведена в разделе “Блок-схема 3: Проверка прав доступа пользователя к объекту” на стр. 182.

Для просмотра частных прав доступа пользователя к объектам библиотек воспользуйтесь командой Показать пользовательский профайл:

DSPUSRPRF *пользовательский-профайл* TYPE(*OBJAUT)

Работать с частными правами доступа пользователя к объектам библиотек и каталогов можно с помощью команды Работа с объектами по частным правам доступа (WRKOBJPVT). Для того чтобы изменить частные права доступа пользователя, выполните команду, управляющую этими правами доступа, такую как Редактировать права доступа к объекту (EDTOBJAUT).

Частные права доступа можно скопировать из одного пользовательского профайла в другой с помощью команды Предоставить права доступа пользователю (GRTUSRAUT). Дополнительная информация приведена в разделе “Копирование прав доступа пользователя” на стр. 173.

Права доступа основной группы

Имена всех объектов, для которых профайл является основной группой, сохраняются в профайле группы.

Список объектов библиотек, для которых профайл является основной группой, можно просмотреть с помощью команды DSPUSRPRF:

DSPUSRPRF *профайл-группы* TYPE(*OBJPGP)

Кроме того, вы можете воспользоваться командой Работа с объектами по основной группе (WRKOBJPGP).

Информация о принадлежности объекта

Так как размер пользовательского профайла влияет на производительность, не рекомендуется присваивать все (или практически все) объекты одному пользовательскому профайлу.

Информация о частных правах доступа к объекту хранится в пользовательском профайле, которому принадлежит этот объект. С помощью этой информации создаются системные меню, позволяющие работать с правами доступа к объектам. Если профайлу принадлежит большое число объектов с различными частными правами доступа, это может привести к снижению производительности создания меню прав доступа к этим объектам. Размер таких профайлов влияет на производительность при работе с правами доступа к объектам и при сохранении и восстановлении профайлов. Кроме того, он может повлиять на выполнение операций в системе. Во избежание этого распределите объекты между несколькими профайлами.

Цифровой идентификатор

Цифровые сертификаты позволяют защитить соединения пользователей и обеспечивают целостность сообщений. Система защиты System i iSeries позволяет применять для идентификации цифровые сертификаты x.509.

API цифровых ИД позволяют создавать, распространять цифровые сертификаты, связанные с пользовательскими профайлами, и управлять ими. В разделе API управления сертификатами подробно описаны следующие API:

- Добавить пользовательский сертификат (QSYADDUC)
- Удалить пользовательский сертификат (QSYRMVUC)
- Просмотреть пользовательский сертификат (QSYLSTUC)
- Найти пользователя сертификата (QSYFNDC)
- Добавить сертификат списка проверки (QSYADDVC)
- Удалить сертификат списка проверки (QSYRMVVC)
- Просмотреть сертификат списка проверки (QSYLSTVC)
- Проверить сертификат списка проверки (QSYCHKVC)
- Анализировать сертификат (QSYPARSC)

Работа с пользовательскими профайлами

В этом разделе описаны команды и меню, применяемые для создания, изменения и удаления пользовательских профайлов операционной системы i5/OS.

Для создания, изменения и удаления пользовательских профайлов необходимы специальные права доступа *SECADM.

Создание пользовательского профайла

Создать пользовательский профайл можно в меню Работа с пользовательскими профайлами (WRKUSRPRF), с помощью команды Создать пользовательский профайл (CRTUSRPRF) или опции Работа с регистрацией пользователей меню SETUP или команды System i Navigator .

Пользователь, создающий пользовательский профайл, становится его владельцем и получает к нему права доступа *ALL. Пользовательский профайл получает права доступа к себе *OBJMGT и *CHANGE. Эти права доступа необходимы для нормальной работы и удалять их не следует.

Права доступа и возможности пользовательского профайла не могут быть шире, чем у пользователя, который создал этот профайл.

Примечание: С помощью команды Создать пользовательский профайл (CRTUSRPRF) нельзя создать пользовательский профайл в независимом пуле дисков. Однако, если пользователь обладает частными правами доступа к объекту из независимого пула дисков, является владельцем такого объекта или входит в состав основной группы этого объекта в независимом пуле дисков, то имя пользовательского профайла хранится в независимом пуле дисков. В случае перемещения независимого пула дисков в другую систему записи о частных правах доступа, принадлежности объектов и основных группах прикрепляются к пользовательскому профайлу с тем же именем в целевой системе. Если в целевой системе нет такого профайла, то он будет создан. Этому профайлу не будут предоставлены специальные права доступа, а его паролю будет присвоено значение *NONE.

Применение команды Работа с пользовательскими профайлами

В команде Работа с пользовательскими профайлами (WRKUSRPRF) можно задать точное имя профайла, задать шаблон имен профайлов или значение *ALL.

Показанное меню зависит от выбранного уровня поддержки. При работе с уровнем поддержки *BASIC появится меню Работа с регистрацией пользователей. Если же задан уровень поддержки *INTERMED, то появится меню Работа с пользовательскими профайлами.

Вы можете задать в команде параметр ASTLVL (уровень поддержки). Если параметр ASTLVL не задан, то система воспользуется значением уровня поддержки из вашего пользовательского профайла.

В меню Работа с пользовательскими профайлами укажите опцию 1 и введите имя создаваемого профайла:

Работа с пользовательскими профайлами

Введите опции и нажмите Enter.

1=Создать 2=Изменить 3=Скопировать 4=Удалить
5=Просмотреть 12=Работа владельца с объектами

Опц	Польз. Профайл	Текст
1	NEWUSER	
—	DPTSM	Отдел сбыта
—	DPTWH	Склад

Будет показано меню Создать пользовательский профайл:

```
                Создать пользовательский профайл (CRTUSRPRF)

Введите опции, нажмите Enter.

Пользовательский профайл . . . . . NEWUSER      Имя
Пароль . . . . . *NONE      Символьное значение, *USRPRF...
Ограничить срок действия пароля . . . . *YES      *NO, *YES
Состояние . . . . . *ENABLED      *ENABLED, *DISABLED
Класс пользователя . . . . . *USER      *USER, *SYSOPR, *PGMR...
Уровень поддержки . . . . . *SYSVAL      *SYSVAL, *BASIC, *INTERMED...
Текущая библиотека . . . . . *CRTDFT      Имя, *CRTDFT
Начальная программа . . . . . *NONE      Имя, *NONE
Библиотека . . . . .          Имя, *LIBL, *CURLIB
Начальное меню . . . . . MAIN      Имя, *SIGNOFF
Библиотека . . . . . QSYS      Имя, *LIBL, *CURLIB
Ограничить возможности . . . . . *NO      *NO, *PARTIAL, *YES
Описание . . . . .
*BLANK
```

В меню Создать пользовательский профайл показаны все поля пользовательского профайла. Для ввода дополнительной информации нажмите клавишу F10 (Дополнительные параметры), а затем - клавишу Page Down. Для просмотра имен параметров нажмите клавишу F11 (Ключевые слова).

Меню Создать пользовательский профайл не позволяет добавить пользователя в системный каталог.

Применение команды Создать пользовательский профайл

Создать пользовательский профайл можно с помощью одноименной команды (CRTUSRPRF). Вы можете указать параметры в командной строке, либо нажать клавишу F4 (Приглашение) для просмотра меню Создать пользовательский профайл.

Применение опции Работа с регистрацией пользователей

Опция Работа с регистрацией пользователей позволяет добавить пользователей в систему.

Выберите в меню SETUP опцию Работа с регистрацией пользователей. В зависимости от уровня поддержки, заданном в вашем пользовательском профайле, вы будет показано меню Работа с пользовательскими профайлами или меню Работа с регистрацией пользователей. Изменить уровень поддержки можно с помощью клавиши F21 (Выбрать уровень поддержки).

В меню Работа с регистрацией пользователей с помощью опции 1 (Добавить) можно добавить в систему нового пользователя.

```
                Работа с регистрацией пользователей

Введите опции и нажмите Enter.
1=Добавить 2=Изменить 3=Скопировать 4=Удалить
5=Просмотреть

Опц   Пользователь   Описание
1     NEWUSER
-     DPTSM           Отдел сбыта
-     DPTWH           Склад
```

Будет показано меню Добавить пользователя:

```

                                Добавить пользователя

Введите варианты и нажмите Enter.

Пользователь. . . . . NEWUSER      Имя
Описание пользователя . .
Пароль. . . . . NEWUSER
Тип пользователя . . . . *USER      Тип, F4 - список
Группа пользователя . . .
*NONE      Имя, F4 - список

Ограничить работу в командной строке  Н          Д=Да, Н=Нет

Библиотека по умолчанию .
      Имя
Принтер по умолчанию . . . . *WRKSTN      Имя, *WRKSTN, F4 - список
Программа, вызываемая при входе в систему . . . . *NONE      Имя, *NONE
Библиотека . . . . .      ФИО
Начальное меню. . . . .
      ФИО Library . . . . .      ФИО
F1=Справка  F3=Выход  F5=Обновить  F12=Отмена

```

Меню **Добавить пользователя** предназначено для системных администраторов, не имеющих технического образования. В нем показаны не все поля пользовательского профайла. Для всех отсутствующих полей применяются значения по умолчанию.

Примечание: В меню **Добавить пользователя** длина имени пользовательского профайла ограничена восемью символами.

Для перехода ко второму меню нажмите Page Down:

```

                                Добавить пользователя

Введите варианты и нажмите Enter.

Программа реакции на клавишу . . *SYSVAL  Library . . . . .

```

Меню **Добавить пользователя** автоматически добавляет в системный каталог запись с ИД, соответствующим имени пользовательского профайла (первые восемь символов), и адресом, соответствующим имени системы.

Копирование пользовательского профайла

Пользовательский профайл можно создать путем копирования другого пользовательского профайла или профайла группы.

Вы можете настроить один из профайлов в группе в качестве шаблона. Затем для создания новых профайлов достаточно будет скопировать первый профайл группы.

Скопировать профайл можно в интерактивном режиме с помощью меню **Работа с регистрацией пользователей** или меню **Работа с пользовательскими профайлами**. Команды для копирования пользовательского профайла не существует.

Понятия, связанные с данным

“Профайлы групп” на стр. 5
Профайл группы - это особый тип пользовательского профайла. Если требуется предоставить одинаковые права доступа нескольким пользователям, то с помощью профайла группы вы можете сделать это за один прием.

Копирование с помощью меню Работа с пользовательскими профайлами

Скопировать профайл можно в меню Работа с пользовательскими профайлами.

В меню Работа с пользовательскими профайлами укажите опцию 3 напротив копируемого профайла. Будет показано меню Создать пользовательский профайл:

```
Создать пользовательский профайл (CRTUSRPRF)
Введите опции, нажмите Enter.
Пользовательский профайл . . . . . Имя
Пароль . . . . . > *USRPRF Имя
Ограничить срок действия пароля . . . . . > *NO *NO, *YES
Состояние . . . . . > *ENABLED *ENABLED,
Класс пользователя . . . . . > *USER *USER,
Уровень поддержки . . . . . > *SYSVAL *SYSVAL,
Текущая библиотека . . . . . > DPTWH Имя,
Начальная программа . . . . . > *NONE Имя,
Библиотека . . . . . Имя,
Начальное меню . . . . . > ICMAIN Имя,
Библиотека . . . . . > ICPGMLIB Имя,
Ограничить возможности . . . . . > *NO *NO,
Описание . . . . .
> 'Отдел хранения'
```

В Меню Создать пользовательский профайл будут показаны все поля исходного пользовательского профайла, кроме следующих:

Пользовательский профайл

Пустое поле. Необходимо указать значение.

Пароль

По умолчанию для команды CRTUSRPRF

Пароль документов

*NONE

Очередь сообщений

*USRPRF

Атрибуты локали задания

*SYSVAL

Локаль

*SYSVAL

User Identification Number

*GEN

Group Identification Number

*NONE

Домашний каталог

*USRPRF

Связь EIM

*NOCHG

Права доступа

*EXCLUDE

Вы можете изменять любые поля в меню Создать пользовательский профайл по своему усмотрению. Частные права доступа исходного профайла не копируются. Внутренние объекты, содержащие параметры пользователя, а также иную информацию о пользователе, не копируются.

Копирование с помощью меню Работа с регистрацией пользователей

Скопировать пользовательский профайл можно также с помощью меню Работа с регистрацией пользователей.

В меню Работа с регистрацией пользователей укажите опцию 3 напротив копируемого профайла. Будет показано меню Скопировать пользователя:

```

                                Скопировать пользователя

Исходный пользователь . : DPTWH
Введите варианты и нажмите Enter.

Пользователь. . . . .
Описание пользователя . . Склад
Пароль. . . . .
Тип пользователя . . . . . USER
Группа пользователя . . .
Доступ к командной строке  Н

Библиотека по умолчанию .
DPTWH
Принтер по умолчанию . . PRT04
Программа, вызываемая при входе в систему . . . . *NONE
Библиотека . . . . .
```

В Меню Добавить пользователя будут показаны все поля исходного пользовательского профайла, кроме следующих:

Пользователь (User)

Пустое поле. Необходимо указать значение. Не более 8 символов.

Пароль

Пустое поле. Если вы не введете значение, профайл будет создан с паролем по умолчанию, указанным в параметре PASSWORD команды CRTUSRPRF.

Все поля в меню Скопировать пользователя можно изменять. Поля, не указанные в меню основного уровня поддержки, будут скопированы из исходного профайла, за следующими исключениями:

Очередь сообщений

*USRPRF

Пароль документов

*NONE

User Identification Number

*GEN

Group Identification Number

*NONE

Связь EIM

*NOCHG

Права доступа

*EXCLUDE

Частные права доступа исходного профайла не копируются.

Копирование частных прав доступа

Скопировать частные права доступа из одного пользовательского профайла в другой можно с помощью команды Предоставить пользователю права доступа (GRTUSRAUT).

Эту возможность не следует применять вместо профайлов групп или списков прав доступа. Копирование прав доступа не позволит вам в дальнейшем управлять скопированными правами доступа и может послужить причиной снижения производительности системы.

Понятия, связанные с данным

“Копирование прав доступа пользователя” на стр. 173

Команда Предоставить права доступа пользователю (GRTUSRAUT) позволяет скопировать все частные права доступа из одного пользовательского профайла в другой.

Изменение пользовательского профайла

Изменить пользовательский профайл можно с помощью опции 2 (Изменить) меню Работа с пользовательскими профайлами или Работа с регистрацией пользователей. Можно также воспользоваться командой Изменить пользовательский профайл (CHGUSRPRF).

Пользователи, которым разрешен ввод команд, могут изменять некоторые параметры своих профайлов с помощью команды Изменить профайл (CHGUSRPRF).

Пользователь не может добавлять в профайл специальные права доступа и дополнительные возможности, которых нет у самого пользователя.

Удаление пользовательских профайлов

Если пользовательскому профайлу принадлежат какие-либо объекты, то его нельзя удалять. Перед его удалением сначала нужно удалить все принадлежащие этому профайлу объекты или передать их другому профайлу.

Нельзя удалить пользовательский профайл, который является профайлом основной группы для каких-либо объектов. При удалении пользовательского профайла с помощью меню промежуточного уровня поддержки, основную группу объектов можно изменить или удалить. С помощью команды WRKOBJPGP можно просмотреть все объекты, для которых профайл является профайлом основной группы.

При удалении пользовательского профайла пользователь будет удален из всех списков рассылки и из системного каталога.

Изменять владельца очереди сообщений пользователя или удалять ее не нужно. Система автоматически удаляет очередь сообщений при удалении профайла.

Нельзя удалить профайл непустой группы. Для просмотра списка членов группы введите команду DSPUSRPRF *имя-профайла-группы* *GRPMBR. Перед удалением профайла группы измените поле GRPPRF или SUPGRPPRF для всех профайлов членов группы.

Применение команды Удалить пользовательский профайл

Вы можете непосредственно вызвать команду Удалить пользовательский профайл (DLTUSRPRF) или воспользоваться опцией 4 (Удалить) в меню Работа с пользовательскими профайлами.

Параметры команды DLTUSRPRF позволяют управлять следующими объектами:

- Все объекты, принадлежащие профайлу.
- Все объекты, для которых профайл является профайлом основной группы
- Связи EIM

Удалить пользовательский профайл (DLTUSRPRF)

Введите опции, нажмите Enter.

Пользовательский профайл > HOGANR Имя
Опция принадлежащих объектов:
 Значение принадлежащего объекта *CHGOWN *NODLT, *DLT, *CHGOWN
Имя профайла для *CHGOWN WILLISR Имя
Опция основной группы:
 Значение основной группы . . . *NOCHG *NOCHG, *PGP
Новая основная группа
Новые права доступа основной группы
Связь EIM *DLT *DLT, *NODLT

Принадлежащие профайлу объекты можно удалить или передать новому владельцу. Для работы с отдельными объектами, принадлежащими профайлу, можно воспользоваться командой Работа с объектами по владельцу (WRKOBJOWN). Вы можете изменить основную группу всех объектов, для которых профайл группы является профайлом основной группы. Для работы с отдельными объектами можно воспользоваться командой Работа с объектами по владельцу (WRKOBJOWN). Меню для обеих команд выглядят одинаково:

Работа владельца с объектами

Пользовательский профайл : HOGANR

Введите опции и нажмите Enter.

2=Изменить права доступа 4=Удалить 5=Показать автора
8=Показать описание 9=Изменить владельца

Опц	Объект	Библиотека	Тип	Атрибут	ASP
4	HOGANR	QUSRSYS	*MSGQ		*SYSBAS
9	QUERY1	DPTWH	*PGM		*SYSBAS
9	QUERY2	DPTWH	*PGM		*SYSBAS

Применение опции Удалить пользователя

Опция Удалить пользователя в меню Работа с регистрацией пользователей позволяет удалить пользовательский профайл.

В меню Работа с регистрацией пользователей укажите опцию 4 (Удалить) напротив удаляемого профайла. Будет показано меню Удалить пользователя:

Удалить пользователя

Пользователь : HOGANR

Описание пользователя . . . : Отдел сбыта

Для удаления этого пользователя введите опцию и нажмите Enter.

1. Передать все объекты этого пользователя другому пользователю.
2. Удалить некоторые объекты пользователя или изменить их владельца

Для того чтобы перед удалением профайла изменить владельца всех объектов, выберите опцию 1. Будет показано меню, в котором вы сможете указать нового владельца.

Для работы с отдельными объектами выберите опцию 2. Будет показано подробное меню Удалить пользователя:

Удалить пользователя

Пользователь : HOGANR
 Описание пользователя . . . : Hogan, Richard - Склад
 Новый владелец Имя, F4 - список

Для удаления пользователя удалите все объекты или измените их владельца. Введите опции и нажмите Enter.
 2=Изменить владельца 4=Удалить 5=Сведения

Опц	Объект	Библиотека	Описание
4	HOGANR	QUSRSYS	Очередь сообщений HOGANR
2	QUERY1	DPTWH	Запрос для отчета
2	QUERY2	DPTWH	Запрос заказов

С помощью показанных на экране опций можно удалить объекты или передать их другому владельцу. Профайл можно будет удалить после того, как список станет пустым.

Notes:

1. Удалить все объекты, принадлежащие пользовательскому профайлу, можно с помощью клавиши F13.
2. Буферные файлы не показаны в меню Работа с объектами по владельцу. Если профайлу принадлежат только буферные файлы, то его можно удалить. После удаления профайла вы сможете с помощью команды Работа с буферными файлами (WRKSPLF) найти и удалить ненужные буферные файлы, принадлежавшие этому пользовательскому профайлу.
3. Объекты, для которых удаленный профайл являлся профайлом основной группы, теперь будут иметь основную группу *NONE.

Работа с объектами по частным правам доступа

С помощью команды Работа с объектами по частным правам доступа (WRKOBJPVT) можно просматривать объекты, к которым у профайла есть частные права доступа, и работать с этими объектами.

Работа с объектами по основной группе

С помощью команды Работа с объектами по основной группе (WRKOBJPGP) можно просматривать объекты, для которых профайл является профайлом основной группы, и работать с этими объектами.

С помощью этого меню можно изменить профайл основную группы или присвоить ей значение *NONE.

Работа с объектами по основной группе

Основная группа : DPTAR
 Введите опции и нажмите Enter.
 2=Редактировать права доступа 4=Удалить 5=Показать права
 8=Показать описание 9=Изменить основную группу

Опц	Объект	Библиотека	Тип	Атрибут	ASP
	CUSTMAST	CUSTLIB	*FILE	*SYSBAS	
	CUSTWRK	CUSTLIB	*FILE	*SYSBAS	
	CUSTLIB	QSYS	*LIB	*SYSBAS	

Включение пользовательского профайла

Если в системных значениях QMAXSIGN и QMAXSGNACN включено блокирование пользовательского профайла после превышения установленного числа неудачных попыток ввода пароля, то может потребоваться включить профайл, изменив состояние профайла на *ENABLED.

Для включения пользовательского профайла нужны специальные права доступа *SECADM и права доступа *OBJMGT и *USE к пользовательскому профайлу. Обычно у системного оператора нет специальных прав доступа *SECADM. Решением является использование простой программы, которая принимает права доступа:

1. Создайте программу на CL, владелец которой имеет специальные права доступа *SECADM и права доступа *OBJMGT и *USE к пользовательским профайлам системы. При создании программы включите принятие прав доступа владельца, указав параметр USRPRF(*OWNER).
2. С помощью команды EDTOBJAUT задайте для программы общие права доступа *EXCLUDE и предоставьте системному оператору права доступа *USE.
3. Оператор может включить профайл командой CALL ENABLEPGM *профайл*.
4. Основная часть программы ENABLEPGM выглядит так:

```
PGM &PROFILE
DCL VAR(&PROFILE) TYPE(*CHAR) LEN(10)
CHGUSRPRF USRPRF(&PROFILE) STATUS(*ENABLED)
ENDPGM
```

Просмотр пользовательских профайлов

Информацию о пользовательских профайлах можно просмотреть и распечатать несколькими способами.

Просмотр отдельного профайла

Просмотреть значения отдельного пользовательского профайла можно с помощью опции 5 (Показать) меню Работа с регистрацией пользователей или Работа с пользовательскими профайлами. Можно также воспользоваться командой Показать пользовательский профайл (DSPUSRPRF).

Просмотр всех профайлов

С помощью команды Показать пользователей с правами доступа (DSPAUTUSR) можно просмотреть или распечатать список всех пользовательских профайлов системы.

Параметр последовательности (SEQ) позволяет сортировать список по именам профайлов и по профайлам группы.

Показать пользователей с правами доступа				
Профайл группы	Пользоват. профайл	Последнее изменение пароля	Нет пароля	Текст
DPTSM	ANDERSR	08/04/0x		Anders, Roger
	VINCENT	09/15/0x		Vincent, Mark
DPTWH	ANDERSR	08/04/0x		Anders, Roger
	HOGANR	09/06/0x		Hogan, Richard
	QUINN	09/06/0x		Quinn, Rose
QSECOFR	JONESS	09/20/0x		Jones, Sharon
	HARRISON	08/29/0x		Harrison, Ken
*NO GROUP	DPTSM	09/05/0x	X	Сбыт
	DPTWH	09/18/0x	X	Склад

С помощью клавиши F11 можно определить, для каких пользовательских профайлов включено применение паролей на различных уровнях.

Показать пользователей с правами доступа

Польз профайл	Групп. профайл	Пароль Посл. измен.	Уровень 0 или 1 Пароль	Уровень 2 или 3 Пароль	Netserver Пароль	Локально Pwd Mgt
ANGELA		04/21/0x	*YES	*NO	*YES	*YES
ARTHUR		07/07/0x	*YES	*YES	*YES	*YES
CAROL1		05/15/0x	*YES	*YES	*YES	*YES
CAROL2		05/15/0x	*NO	*NO	*NO	*NO
CHUCKE		05/18/0x	*YES	*NO	*YES	*YES
DENNISS		04/20/0x	*YES	*NO	*YES	*YES
DPORTER		03/30/0x	*YES	*NO	*YES	*YES
GARRY		08/04/0x	*YES	*YES	*YES	*YES
JANNY		03/16/0x	*YES	*NO	*YES	*YES

Тип показа пользовательского профайла

Команда Показать пользовательский профайл (DSPUSRPRF) позволяет работать с меню и списками различных типов.

- Некоторые меню и списки доступны лишь отдельным профайлам. Остальные можно распечатать для всех профайлов или для определенного шаблона имен профайлов.
- Для некоторых меню можно создать файл вывода, указав параметр (*OUTFILE). Для создания отчетов на основании полученного вывода можно воспользоваться утилитой Query или какой-либо программой. В “Анализ пользовательских профайлов” на стр. 320 приведены варианты отчетов.

Типы отчетов пользовательского профайла

Создать отчеты пользовательского профайла можно с помощью команды Печать пользовательского профайла (PRTUSRPRF) или Проанализировать пароль по умолчанию (ANZDFTPWD).

- Печать пользовательских профайлов (PRTUSRPRF)

Эта команда создает отчеты с информацией о пользовательских профайлах в системе. Можно напечатать четыре варианта отчетов. Эти отчеты содержат информацию о правах доступа, о среде, о пароле и об уровне пароля.

- Анализировать пароли по умолчанию (ANZDFTPWD)

Эта команда печатает отчет о всех пользовательских профайлах системы, которые имеют пароль по умолчанию, и позволяет принимать меры против наличия в системе таких профайлов. Пароль по умолчанию совпадает с именем профайла.

Пользовательские профайлы системы с паролем по умолчанию можно отключить, а для их паролей задать опцию истекшего срока действия.

Переименование пользовательского профайла

Переименование пользовательского профайла в системе не предусмотрено. Можно создать новый профайл с теми же правами доступа, но с другим именем.

Однако новому профайлу можно передать не всю информацию. Ниже приведены примеры объектов, которые нельзя передать:

- Буферные файлы.
- Внутренние объекты, содержащие параметры для пользователя и иную информацию о пользователе будут утеряны.
- Цифровые сертификаты с именем пользователя будут аннулированы.
- Информацию uid и gid, содержащуюся в интегрированной файловой системе, изменить нельзя.
- Могут возникнуть проблемы при изменении информации приложений, содержащей имя пользователя.

У приложений, запускаемых пользователем, могут быть профайлы приложений. Создание нового пользовательского профайла i5/OS для изменения имени пользователя не приведет к изменению профайлов приложений. Примером профайла приложения может служить профайл Lotus Notes.

Следующий пример описывает создание нового профайла с новым именем и старыми правами доступа. Старое имя профайла - SMITHM, а новое имя пользовательского профайла - JONESM:

1. Скопируйте старый профайл (SMITHM) в новый профайл (JONESM) с помощью опции копирования в меню Работа с регистрацией пользователей.
2. С помощью команды Предоставить права доступа пользователю (GRTUSRAUT) предоставьте JONESM те же частные права доступа, что и SMITHM:
GRTUSRAUT JONESM REFUSER(SMITHM)
3. С помощью команды Работа с объектами по основной группе (WRKOBJPGP) измените основную группу всех объектов, для которых профайл SMITHM является профайлом основной группы:
WRKOBJPGP PGP(SMITHM)
Укажите опцию 9 для всех объектов, основную группу которых нужно изменить, и задайте в командной строке опцию NEWPGP(JONESM).

Примечание: gid JONESM необходимо присвоить с помощью параметра GID команды Создать или Изменить пользовательский профайл (CRTUSRPRF или CHGUSRPRF).

4. С помощью команды Показать пользовательский профайл (DSPUSRPRF) просмотрите пользовательский профайл SMITHM:
DSPUSRPRF USRPRF(SMITHM)

Запишите uid и gid профайла SMITHM.

5. Передайте все объекты пользовательскому профайлу JONESM, а затем с помощью опции 4 (Удалить) меню Работа с регистрацией пользователей удалите профайл SMITHM.
6. С помощью команды Изменить пользовательский профайл (CHGUSRPRF) измените uid и gid JONESM на uid и gid SMITHM:
CHGUSRPRF USRPRF(JONESM) UID(uid-из-SMITHM)
GID(gid-из-SMITHM)

Если JONESM является владельцем объектов из каталога, то изменить uid и gid с помощью команды CHGUSRPRF нельзя. В этом случае можно воспользоваться API QSYCHGID.

Работа со средствами контроля пользователей

С помощью команды Изменить контроль пользователей (CHGUSRAUD) можно настроить параметры контроля пользователей.

Для выполнения этой команды необходимы специальные права доступа *AUDIT.

Изменить контроль пользователей (CHGUSRAUD)

Введите опции, нажмите Enter.

```
Пользовательский профайл . . . . . HOGANR
+ для доп. значений JONES
Значение контроля объекта . . . *SAME
Контроль действий пользователя . . . *CMD
+ для доп. значений *SERVICE
```

С помощью списка пользовательских профайлов можно настроить параметры контроля сразу для нескольких пользователей.

У параметра AUDLVL (контроль действий пользователя) может быть несколько значений. Указываемые значения не добавляются к текущим значениям параметра AUDLVL, а заменяют их.

При наличии специальных прав доступа *ALLOBJ или *AUDIT можно просмотреть параметры контроля пользователя с помощью команды Показать пользовательский профайл (DSPUSRPRF).

Работа с профайлами в программах CL

В этом разделе описана работа с профайлами в программах CL.

Программы CL могут получать информацию о пользовательских профайлах. Для этого в программе можно вызвать команду Получить пользовательский профайл (RTVUSRPRF). Команда вернет запрошенные атрибуты профайла в переменные, соответствующие полям пользовательского профайла. В этом разделе приведены описания полей пользовательского профайла и указана длина полей команды RTVUSRPRF. Иногда целочисленные поля могут содержать нечисловое значение. Например, поле максимального объема памяти (MAXSTG) определено как целочисленное поле, но может принимать значение *NOMAX. В электронной справке описаны значения, возвращаемые командой RVTUSRPRF в том случае, если целочисленному полю присвоено нечисловое значение.

Пример применения команды RTVUSRPRF приведен в программе “Работа с программой подтверждения паролей” на стр. 64.

В программе CL можно также использовать команды CRTUSRPRF и CHGUSRPRF. Переменные для параметров этих команд нужно определить как символьные поля, соответствующие меню Создать пользовательский профайл. Размеры переменных могут отличаться от размеров полей.

Пароль пользователя получить нельзя, так как он зашифрован с помощью алгоритма одностороннего шифрования. Если вы хотите, чтобы пользователь перед получением доступа к конфиденциальной информации вводил пароль заново, вы можете использовать в программе команду Проверить пароль (CHKPWD). Система сравнит введенный пароль с паролем пользователя и в случае несовпадения отправит программе аварийное сообщение.

Точки выхода пользовательского профайла

Для выполнения конкретных операций над пользовательским профайлом можно создавать собственные программы выхода. При регистрации программ выхода в точке выхода для работы с пользовательским профайлом вы будете получать уведомления о создании, изменении, удалении или восстановлении профайла.

При получении такого уведомления программа выхода сможет выполнить следующие действия:

- Получить информацию о пользовательском профайле
- Зарегистрировать только что созданный пользовательский профайл в системном каталоге
- Создать для пользовательского профайла необходимые объекты

Примечание: Перед вызовом программы выхода все принятые права доступа будут отключены. Это означает, что у программы выхода может не оказаться прав доступа к объекту пользовательского профайла.

Информация, связанная с данной

Программы выхода

IBM, поставляемые пользовательские профайлы

Некоторые пользовательские профайлы поставляются вместе с программным обеспечением. Такие пользовательские профайлы, поставляемые IBM, являются владельцами объектов многих системных функций. Кроме того, некоторые функции системы выполняются от имени пользовательских профайлов, поставляемых IBM.

Профайл системного администратора (QSECOFR) поставляется для всех систем с одним и тем же паролем, чтобы позволить установить систему при первом включении. Однако профайл QSECOFR поставляется с истекшим сроком действия пароля. В новых системах после первого входа в систему под именем QSECOFR необходимо будет сменить пароль.

При установке нового выпуска операционной системы пароли профайлов, поставляемых IBM, не изменяются. Если профайлы, такие как QPGMR и QSYSOPR имеют пароли, то эти пароли не будут автоматически изменены на *NONE.

Полный список пользовательских профайлов, поставляемых IBM, и значений их полей приведен в документе Приложение В, “Пользовательские профайлы, поставляемые IBM”, на стр. 337.

Примечание: Все пользовательские профайлы, поставляемые IBM, за исключением QSECOFR, поставляются с паролем *NONE и не предполагают входа в систему. Эти профайлы используются операционной системой IBM i5/OS. В связи с этим, не рекомендуется входить в систему под управлением этих профайлов или передавать им объекты других пользователей.

Понятия, связанные с данным

“Пользовательские профайлы, поставляемые IBM” на стр. 272

Задачи контроля пользовательских профайлов, поставляемых IBM, выполняются посредством проверки их паролей.

Изменение паролей для пользовательских профайлов, поставляемых IBM

Для входа в систему под управлением одного из профайлов, поставляемых IBM, можно изменить пароль этого профайла с помощью команды CHGUSRPRF или с помощью опции меню SETUP.

Для защиты системы для всех профайлов, поставляемых IBM, кроме QSECOFR должен быть задан пароль *NONE. Не допускайте задания тривиальных паролей для профайла QSECOFR.

Изменение пароля для профайлов IBM

Введите ниже новый пароль для пользователя IBM, введите пароль еще раз, чтобы подтвердить изменения, нажмите Enter.

Новый пароль системного администратора (QSECOFR) . .
Новый пароль (подтверждение)
.

Новый пароль системного оператора (QSYSOPR)
Новый пароль (подтверждение)
.

Новый пароль программиста (QPGMR)
Новый пароль (подтверждение)
.

Новый пароль пользователя (QUSER)
Новый пароль (подтверждение)
.

Новый пароль службы (QSRV)
Новый пароль (подтверждение)
.

Для того чтобы изменить дополнительные пароли, нажмите Page Down:

Изменение пароля для профайлов IBM

Введите ниже новый пароль для пользователя IBM, введите изменения и нажмите Enter.

Новый основной служебный пароль (QSRVBAS)
Новый пароль (подтверждение)
.

Работа с ИД пользователей сервисных средств

Появился ряд дополнений и расширений, сделавших применение сервисных средств более простым и удобным.

- **Системный инструментарий (SST)**

С помощью системного инструментария (SST) можно управлять ИД пользователей сервисных средств и создавать их. Для этого в главном меню SST выберите опцию 8 (Работа с пользователями сервисных средств). Теперь для сброса паролей, предоставления или аннулирования прав доступа или создания ИД пользователя сервисных средств не нужно обращаться к специальным сервисным средствам (DST).

Примечание: Информацию о сервисных средствах вы можете найти в справочной системе Information Center.

- **Эффективное управление паролями**

Сервер поставляется с ограниченными возможностями изменения паролей по умолчанию и паролей с истекшим сроком действия. Это означает, что изменить ИД пользователя сервисных средств с паролем по умолчанию или с истекшим паролем нельзя ни с помощью API Изменить ИД пользователя сервисных средств (QSYCHGDS), ни с помощью SST. Это можно сделать только через DST. При этом вы можете изменить настройку и разрешить изменение паролей с истекшим сроком действия и паролей по умолчанию. Кроме того, с помощью новых прав доступа для Запуска сервисных средств (STRSST) можно создать новый ИД пользователя сервисных средств, который будет иметь доступ к DST, но не будет иметь доступ к SST.

- **Изменения терминологии**

Документация была изменена в соответствии с терминологией сервисных средств. Теперь термин ИД пользователя сервисных средств заменяет собой все остальные термины, такие как пользовательские профайлы DST, ИД пользователей DST, профайлы пользователей сервисных средств и их вариации.

Понятия, связанные с данным

“Пользовательские профайлы, поставляемые IBM” на стр. 272

Задачи контроля пользовательских профайлов, поставляемых IBM, выполняются посредством проверки их паролей.

Информация, связанная с данной

Управление ИД пользователей сервисных средств

Системный пароль

Системный пароль применяется для изменения модели системы, подтверждения условий обслуживания и изменения владельца. Если в системе произошли соответствующие изменения, то при выполнении IPL может быть показано приглашение для ввода системного пароля.

Глава 5. Защита ресурсов

В этом разделе описаны все компоненты защиты ресурсов и приведена информация об их совместном применении для защиты информации в системе. Кроме того, здесь вы сможете найти сведения о настройке защиты ресурсов с помощью команд и меню CL.

Защита ресурсов позволяет ограничить круг пользователей, которым разрешено использовать объекты в системе, а также набор операций, которые разрешено выполнять над этими объектами.

В разделе Глава 7, “Разработка схем защиты”, на стр. 231 описаны различные подходы к организации защиты ресурсов и указано, каким образом они влияют на разработку приложений и производительность системы.

В разделе “Как система проверяет права доступа” на стр. 177 приведены подробные блок-схемы процедуры проверки прав доступа в системе и примечания к ним. Они пригодятся вам при чтении следующей информации.

Понятия, связанные с данным

“Защита ресурсов” на стр. 5

Разрешение на работу с объектом называется *правами доступа*. Защита ресурсов в операционной системе i5/OS позволяет настроить права доступа к объектам и указать, кому и как будет разрешено работать с объектами.

“Общие рекомендации по проектированию защиты” на стр. 232

Отсутствие сложных решений в реализации защиты системы позволяет значительно упростить управление средствами защиты и контроль за их применением. Кроме того, это существенно повышает производительность приложений и операций резервного копирования.

Определение субъектов доступа к информации

Права доступа можно предоставить отдельным пользователям, группам пользователей или всем пользователям.

Примечание: Иногда права доступа пользователя называются **полномочиями**.

Набор пользователей, которым разрешено использовать объект, можно определить несколькими способами:

Общие права доступа:

Общие права доступа предоставляются всем пользователям, которым разрешено работать в системе. Такие права доступа задаются для всех объектов системы, хотя они могут принимать значение *EXCLUDE. Общие права доступа к объекту применяются в том случае, если не заданы права доступа для более узкой группы пользователей.

Частные права доступа:

Вы можете определить конкретные права на использование объекта (или запретить его использование). Эти права доступа можно предоставить отдельному пользовательскому профайлу или профайлу группы. **Частные права доступа** - это все права доступа к объекту, за исключением общих прав доступа, принадлежности объекта и прав доступа основной группы.

Права доступа пользователей:

Права на использование объектов системы можно предоставлять отдельным пользовательским профайлам. Такие права доступа представляют собой одну из разновидностей частных прав доступа.

Права доступа групп:

Права на использование объектов системы можно предоставлять профайлам групп. Любой элемент группы получает права доступа, заданные для группы, если для него не определены права доступа пользователя. Права доступа группы также относятся к частным правам доступа.

Принадлежность объекта:

У любого объекта системы есть владелец. По умолчанию владельцу предоставлены права доступа *ALL по отношению к принадлежащему ему объекту. Эти права доступа можно изменить или удалить. Права доступа владельца объекта не относятся к категории частных прав доступа.

Права доступа основной группы:

Для объекта можно определить основную группу и ее права доступа. Права доступа основной группы хранятся вместе с объектом и в некоторых случаях обеспечивают более высокую производительность, чем частные права доступа, предоставленные профайлу группы. Основной группой объекта можно назначить только тот профайл, которому присвоен идентификатор группы (gid). Права доступа основной группы не относятся к категории частных прав доступа.

Определение режима доступа к информации

Можно указать, какие операции разрешены с объектами, данными и полями.

Права доступа определяют разрешенный способ доступа к объекту. Для выполнения различных операций требуются разные типы прав доступа.

Примечание: В некоторых случаях заданные для объекта права доступа называются **режимом доступа к объекту**.

Права доступа к объекту подразделяются на три категории:

1. **Права доступа к объекту** определяют операции, которые разрешено выполнять над всем объектом.
2. **Права доступа к данным** определяют операции, которые разрешено выполнять над содержимым объекта.
3. **Права доступа к полям** определяют операции, которые разрешено выполнять над отдельными полями данных.

В разделе Табл. 115 описаны существующие типы прав доступа и приведены примеры их применения. В большинстве случаев для получения доступа к объекту требуется наличие определенного сочетания прав доступа к объекту, данным и полям. В разделе Приложение D, “Права доступа, требуемые для объектов, используемых командами”, на стр. 359 приведена информация о правах доступа, необходимых для выполнения различных функций.

Таблица 115. Описание типов прав доступа

Права доступа	Имя	Разрешенные функции
<i>Права доступа к объекту:</i>		
*OBJOPR	Операционные права доступа к объекту	Просмотр описания объекта. Применение объекта в тех рамках, которые определяются правами доступа пользователя к данным.
*OBJMGT	Управление объектом	Настройка параметров защиты объекта. Перемещение и переименование объекта. Все функции, допустимые для *OBJALTER и *OBJREF.
*OBJEXIST	Существование объекта	Удаление объекта. Освобождение памяти объекта. Сохранение и восстановление объекта ¹ . Передача принадлежности объекта.
*OBJALTER	Изменение объекта	Добавление, очистка, инициализация и реорганизация элементов файла базы данных. Изменение и добавление атрибутов файлов базы данных: добавление и удаление триггеров. Изменение атрибутов пакетов SQL.

Таблица 115. Описание типов прав доступа (продолжение)

Права доступа	Имя	Разрешенные функции
*OBJREF	Обращение к объекту	Настройка файла базы данных в качестве родительской таблицы в ограничении по ссылкам. Предположим, вам нужно определить правило, согласно которому заказ может быть добавлен в файл CUSORD только при условии, что в файле CUSMAS есть запись о заказчике. Для определения такого правила необходимо получить права доступа *OBJREF к файлу CUSMAS.
*AUTLMGT	Управление списком прав доступа	Добавление и удаление пользователей и их прав доступа в списке прав доступа ² .
<i>Права доступа к данным:</i>		
*READ	Чтение	Просмотр содержимого объекта, в том числе просмотр записей файла.
*ADD	Добавление	Добавление записей в объект, в том числе добавление сообщений в очередь и добавление записей в файл.
*UPD	Обновление	Изменение записей в объекте, в том числе изменение записей файла.
*DLT	Удаление	Удаление записей из объекта, в том числе удаление сообщений из очереди и записей из файла.
*EXECUTE	Выполнение	Выполнение программы, служебной программы или пакета SQL. Поиск объекта в библиотеке или каталоге.
<i>Права доступа к полям:</i>		
*MGT	Управление	Настройка параметров защиты поля.
*ALTER	Изменение	Изменение атрибутов поля.
*REF	Справочник	Добавление поля в родительский ключ в ограничении по ссылкам.
*READ	Чтение	Доступ к содержимому поля. Например, просмотр содержимого поля.
*ADD	Добавление	Добавление записей к данным, в том числе добавление информации в поле.
*UPDATE	Обновление	Изменение содержимого поля.
¹	Если у пользователя есть специальные права на сохранение системы (*SAVSYS), то для сохранения и восстановления объекта права к существованию объекта не нужны.	
²	За дополнительной информацией обратитесь к разделу “Управление списком прав доступа” на стр. 145.	

Задачи, связанные с данной

“Переход на уровень 30 с более низкого уровня” на стр. 13

При переходе на уровень защиты 30 с более низкого уровня пользовательские профайлы изменяются после очередной IPL для обновления специальных прав доступа.

Ссылки, связанные с данной

“Права доступа группы” на стр. 103

Если пользовательский профайл входит в состав группы и указан параметр OWNER(*USRPRF), то поле Права доступа группы позволяет управлять правами доступа к объектам, созданным этим пользователем, которые получает профайл группы.

Часто используемые права доступа

Права доступа к данным и объектам можно объединить в наборы.

Некоторые наборы прав доступа к данным и объекту особенно часто используются при выполнении операций над объектом. Такие системные наборы прав доступа (*ALL, *CHANGE, *USE) можно указывать вместо перечня необходимых прав доступа к объекту. Права доступа *EXCLUDE не означают отсутствие прав доступа. Это значение явно запрещает доступ к объекту. Отсутствие прав доступа означает, что пользователю будут предоставлены общие права доступа к объекту. В Табл. 116 описаны системные наборы прав доступа, которые можно указывать в командах и меню в качестве прав доступа к объекту.

Таблица 116. Системные права доступа

Права доступа	*ALL	*CHANGE	*USE	*EXCLUDE
<i>Права доступа к объекту</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
<i>Права доступа к данным</i>				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

В Табл. 117 описаны дополнительные системные права доступа, которые можно указывать в командах WRKAUT и CHGAUT:

Таблица 117. Системные права доступа

Права доступа	*RWX	*RW	*RX	*R	*WX	*W	*X
<i>Права доступа к объекту</i>							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
<i>Права доступа к данным</i>							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

В лицензионной программе LAN Server для управления правами доступа применяются списки управления доступом. Права доступа пользователей иногда называются **разрешениями**. В Табл. 118 на стр. 141 перечислены права доступа к данным и объектам, соответствующие разрешениям LAN Server:

Таблица 118. Разрешения LAN Server

Права доступа	Разрешения LAN Server
*EXCLUDE	Нет
<i>Права доступа к объекту</i>	
*OBJOPR	См. примечание 1
*OBJMGT	Разрешение
*OBJEXIST	Создание, удаление
*OBJALTER	Атрибут
*OBJREF	Нет эквивалента
<i>Права доступа к данным</i>	
*READ	Чтение
*ADD	Создание
*UPD	Запись
*DLT	Удаление
*EXECUTE	Выполнение

¹ Пользователю неявно предоставлены права доступа *OBJOPR, если в списке управления доступом не задано значение NONE.

Определение условий доступа к информации

Защиту ресурсов можно настроить на уровне отдельных объектов системы. Кроме того, защиту можно настроить на уровне групп объектов, используя параметры защиты библиотеки или список прав доступа.

Защита библиотек

Защита библиотек обеспечивает конфиденциальность информации.

Большинство объектов системы хранятся в библиотеках. Для получения доступа к объекту необходимо иметь права доступа к самому объекту и к его библиотеке. Для выполнения большинства операций, в том числе для удаления объекта, достаточно наличия прав доступа *USE к библиотеке объекта (дополнительно к необходимым правам доступа к объекту). Для создания объекта необходимы права доступа *ADD к библиотеке объекта. В разделе Приложение D, “Права доступа, требуемые для объектов, используемых командами”, на стр. 359 указано, какие права доступа к объектам и их библиотекам необходимы для выполнения команд CL.

Защита библиотек - это сравнительно простой способ защиты информации. Так, для защиты конфиденциальной информации группы приложений можно сделать следующее:

- Сохранить все конфиденциальные файлы группы приложений в одной библиотеке.
- Убедиться, что для всех объектов библиотеки, применяемых приложениями, установлены достаточные общие права доступа (*USE или *CHANGE).
- Запретить всем пользователям доступ к библиотеке (задать общие права доступа *EXCLUDE).
- Предоставить некоторым группам или отдельным пользователям права доступа к библиотеке (*USE или *ADD, в зависимости от требований приложения).

Хотя защита библиотек - это простой и эффективный способ защиты информации, он не обеспечивает достаточный уровень защиты для секретных данных. Защита секретных объектов должна настраиваться индивидуально или обеспечиваться списком прав доступа, а не опираться на защиту библиотеки.

Понятия, связанные с данным

“Планирование библиотек” на стр. 236

Структура библиотеки аналогична структуре каталога, позволяющего искать размещенные в нем объекты. Способ объединения информации приложения в библиотеки и управления библиотеками зависит от большого числа факторов.

Защита библиотек и списки библиотек

При добавлении библиотеки в список библиотек пользователя права доступа пользователя к библиотеке сохраняются вместе со списком.

Права доступа пользователя к библиотеке продолжают действовать на протяжении всего времени выполнения задания, даже если они будут аннулированы за это время.

При обращении к объекту, в качестве библиотеки которого задано значение *LIBL, права доступа к библиотеке проверяются с помощью списка библиотек. Когда имя объекта указывается полностью, проверяются текущие права доступа пользователя к библиотеке, даже если эта библиотека включена в состав списка библиотек пользователя.

Внимание: Если при добавлении библиотеки в список пользователь применяет принятые права доступа, то права доступа к этой библиотеке сохраняются у пользователя и после прекращения использования принятых прав доступа. Потенциально это позволяет обойти защиту. Все записи, добавленные в пользовательский список библиотек программой, применяющей принятые права доступа, должны быть удалены до завершения работы этой программы.

Кроме того, потенциальную угрозу представляют те приложения, которые применяют списки библиотек вместо точных имен библиотек. Пользователь, которому разрешено применять команды для работы со списками библиотек, потенциально может модифицировать программу.

Ссылки, связанные с данной

“Списки библиотек” на стр. 218

Список библиотек задания определяет набор библиотек, просматриваемых при поиске, и порядок просмотра библиотек.

Права доступа к полям

Для файлов базы данных можно указать права доступа к полям.

В этой версии можно задавать права доступа к отдельным полям файла базы данных. Поддерживаются права доступа Management, Alter, Reference, Read, Add и Update. Управлять этими правами доступа можно только с помощью операторов GRANT и REVOKE языка SQL. Просмотреть такие права доступа можно с помощью команд Показать права доступа к объекту (DSPOBJAUT) и Редактировать права доступа к объекту (EDTOBJAUT). Обратите внимание, что команда EDTOBJAUT позволяет просматривать права доступа к полям, но не редактировать их.

```

Показать права доступа к объекту
Объект . . . . . : PLMITXT      Владелец . . . . . : PGMR1
Библиотека . . . : RLN          Основная группа . . : DPTAR
Тип объекта . . . : *FILE       Устройство ASP . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : *NONE
Права -----Данные-----
Пользоват  Группы   к объекту Чтение Добав Обнов Удаление Выполнен
*PUBLIC    *CHANGE    X      X      X      X      X
PGMR1      *ALL       X      X      X      X      X
USER1      *USE       X
USER2      USER DEF   X
USER3      USER DEF   X      X

Для продолжения нажмите Enter

F3=Выход  F11=Показать сведения  F12=Отмена
F16=Показать права доступа к полям

```

Рисунок 4. Меню Показать права доступа к объекту с опцией F16=Показать права доступа к полям. Эта опция доступна в том случае, если для полей файла базы данных заданы права доступа.

```

Показать права доступа к полям
Объект . . . . . : PLMITXT      Владелец . . . . . : PGMR1
Library . . . . . : RLN          Основная группа . . : *NONE
Тип объекта . . . : *FILE
Права -----Права доступа к полям-----
Поле      Пользов к объекту Упр  Измен Обр Чтение Доб  Обновл
Field3    PGMR1   *ALL     X    X    X    X    X    X
          USER1   *Use     X
          USER2   USER DEF X
          USER3   USER DEF X
          *PUBLIC *CHANGE X    X    X
Field4    PGMR1   *ALL     X    X    X    X    X
          USER1   *Use     X
          USER2   USER DEF X
          USER3   USER DEF X
          *PUBLIC *CHANGE X    X    X
                                     Еще

Для продолжения нажмите Enter.
F3=Выход F5=Обновить F12=Отмена F16=Повторить переход F17=Перейти к

```

Рисунок 5. Меню Показать права доступа к полям. При нажатии клавиши "F17=Перейти к" появится приглашение Перейти к. При нажатии F16 будет повторно выполнена предыдущая операция перехода.

Права доступа к полям предусматривают следующие опции:

- В команде Печатать частные права доступа (PRTPVTAUT) предусмотрено поле, указывающее, заданы ли права доступа для полей файла.
- В команде Показать права доступа к объекту (DSPOBJAUT) предусмотрен параметр Тип прав доступа, позволяющий просмотреть права доступа к объекту, права доступа к полям или все права доступа. Если тип объекта отличен от *FILE, то можно просмотреть только поля доступа к объекту.
- В выводе API Показать пользователей с доступом к объекту (QSYLUSRA) указывается, заданы ли права доступа для полей файла.
- Команда Предоставить права доступа пользователю (GRTUSRAUT) не предоставляет пользователю права доступа к полям.

- Если в качестве модельного объекта и в качестве целевого объекта предоставления прав в команде GRTOBJAUT заданы файлы базы данных, то права доступа к полям с совпадающими именами будут полностью скопированы.
- При удалении прав доступа пользователя к файлу базы данных удаляются все права доступа к полям этого файла.

Защита при работе со средой System/38

В этом разделе приведена информация о защите при работе в среде System/38.

Применение программ CL типа CLP38 в среде System/38 представляет потенциальную угрозу. Если в меню ввода команд System/38 или в программе CL типа CLP38 вызывается команда, библиотека которой не указана, то в первую очередь поиск команды выполняется в библиотеке QUSER38 (если она существует). После этого поиск выполняется в библиотеке QSYS38. Программист или любой осведомленный об этом пользователь может подменить команду, расположенную в библиотеке из списка библиотек, своей командой, разместив ее в одной из двух указанных библиотек.

Библиотека QUSER38 не поставляется вместе с операционной системой. Однако ее может создать любой пользователь, у которого есть права на создание библиотек.

Информация, связанная с данной



System/38 Environment Programming

Рекомендации по применению среды System/38 Environment

В это разделе приведены рекомендации по работе в среде System/38.

Для защиты системы от потенциальной угрозы, которую представляют среда System/38 и программы CL типа CLP38, рекомендуется принять следующие меры:

- Узнайте текущие общие права доступа к библиотеке QSYS38. Если они равны *ALL или *CHANGE, то измените их на значение *USE.
- Узнайте текущие общие права доступа к библиотеке QUSER38. Если они равны *ALL или *CHANGE, то измените их на значение *USE.
- Если библиотеки QUSER38 и QSYS38 не существуют, то создайте их с общими правами доступа *USE. Это не даст злоумышленнику возможность создать одну из этих библиотек и предоставить себе расширенные права доступа к этой библиотеке.

Защита каталога

Защита каталогов обеспечивает конфиденциальность информации.

Для обращения к объекту их каталога необходимы права доступа ко всем каталогам, входящим в состав пути к объекту. Кроме того, пользователю должны быть предоставлены права доступа к объекту, необходимые для выполнения запрошенной операции.

Защиту каталогов можно использовать так же, как и защиту библиотек. Ограничьте доступ к каталогам и установите общие права доступа для объектов каталога. Максимально сократив число владельцев частных прав доступа к объектам каталога, вы можете повысить скорость проверки прав доступа.

Защита списка прав доступа

Список прав доступа позволяет объединить объекты со схожими требованиями к защите.

Фактически список прав доступа представляет собой список пользователей с указанием прав доступа, которые предоставлены этим пользователям по отношению к объектам, защищенным с помощью списка.

Каждому пользователю можно предоставить свой набор прав доступа к объектам. Когда пользователю предоставляются права доступа к списку прав доступа, фактически ему предоставляются **частные права доступа** к списку.

Список прав доступа может применяться и для определения общих прав доступа к объектам. Если общие права доступа к объекту равны *AUTL, то эти права доступа считываются из списка прав доступа.

Объект списка прав доступа применяется системой как одно из средств управления. Фактически он содержит список всех объектов, для защиты которых применяется список прав доступа. Эта информация применяется для создания меню просмотра и редактирования объектов списка прав доступа.

Список прав доступа нельзя применять для защиты пользовательского профайла или другого списка прав доступа. С каждым объектом можно связать только один список прав доступа.

Задавать и удалять связанный с объектом список прав доступа может только владелец объекта, пользователь со специальными правами доступа ко всем объектам (*ALLOBJ) и пользователь со всеми правами доступа к объекту (*ALL).

Список прав доступа может применяться для защиты объектов из системной библиотеки (QSYS). Однако имя этого списка будет храниться вместе с объектом. В некоторых случаях при установке нового выпуска операционной системы заменяются все объекты из библиотеки QSYS. При этом вся информация о списках прав доступа, связанных с объектами, удаляется.

Примеры применения списков прав доступа приведены в разделе “Преимущества списка прав доступа” на стр. 174.

Управление списком прав доступа

Для списков прав доступа можно задавать особые операционные права доступа, которые называются правами на управление списком прав доступа (*AUTLMGT).

Пользователям с правами доступа *AUTLMGT разрешено добавлять и удалять права доступа пользователей в списке прав доступа, а также изменять права доступа пользователей. Сами по себе права доступа *AUTLMGT не позволяют связывать список с новыми объектами или удалять объекты из списка.

Пользователь с правами доступа *AUTLMGT может предоставить другим пользователям права доступа не выше того уровня, который предоставлен ему самому. Для примера предположим, что пользователю USERA предоставлены права доступа *CHANGE и права доступа *AUTLMGT по отношению к списку прав доступа CPLIST1. USERA может добавить пользователя USERB в список CPLIST1 и предоставить ему права доступа *CHANGE или права доступа более низкого уровня. USERA не может предоставить пользователю USERB права доступа *ALL по отношению к CPLIST1, так как ему самому не предоставлены права доступа *ALL.

Пользователь с правами доступа *AUTLMGT может удалить права доступа другого пользователя, если его уровень прав доступа к списку не ниже уровня прав доступа удаляемого пользователя. Если пользователю USERC предоставлены права доступа *ALL к списку CPLIST1, то USERA не может удалить USERC из списка, так как USERA предоставлены только права доступа *CHANGE и *AUTLMGT.

Применение списка прав доступа для защиты объектов, поставляемых IBM

В этом разделе описано использование списка прав доступа для защиты объектов, поставляемых IBM. Например, с его помощью можно ограничить круг пользователей, которым разрешено применять некоторые команды.

Объекты из всех поставляемых фирмой IBM библиотек, за исключением библиотек QUSRSYS и QGPL, заменяются при установке нового выпуска операционной системы. При этом связь между такими объектами и списками прав доступа теряется. Кроме того, при восстановлении всей системы теряется связь между объектами из библиотеки QSYS и списками прав доступа, применяемыми для их защиты. После установки

нового выпуска или восстановления системы необходимо вызвать команду EDTOBJAUT или GRTOBJAUT для восстановления связей между поставляемыми фирмой IBM объектами и списками прав доступа.

Права доступа к новым объектам библиотеки

Можно указать права доступа к новым объектам библиотеки.

У любой библиотеки есть параметр CRTAUT (права при создании). Этот параметр определяет общие права доступа, которые по умолчанию устанавливаются для новых объектов библиотеки при их создании. Общие права доступа к создаваемому объекту задаются в параметре AUT команды создания. Если параметру AUT присвоено значение *LIBCRTAUT (значение по умолчанию для большинства команд), то для объекта устанавливаются те общие права доступа, которые заданы в параметре CRTAUT библиотеки.

Для примера предположим, что параметру CRTAUT библиотеки CUSTLIB присвоено значение *USE. Обе указанные ниже команды создают область данных DTA1 с общими правами доступа *USE:

- Если задан параметр AUT:
CRTDTAARA DTAARA(CUSTLIB/DTA1) +
TYPE(*CHAR) AUT(*LIBCRTAUT)
- Если параметру AUT присвоено значение по умолчанию (*LIBCRTAUT):
CRTDTAARA DTAARA(CUSTLIB/DTA1) +
TYPE(*CHAR)

По умолчанию параметру библиотеки CRTAUT присвоено значение *SYSVAL. При этом всем объектам, создаваемым в библиотеке с параметром AUT(*LIBCRTAUT), присваиваются те общие права доступа, которые заданы в системном значении QCRTAUT. Системное значение QCRTAUT поставляется со значением *CHANGE. Для примера предположим, что параметру CRTAUT библиотеки ITEMLIB присвоено значение *SYSVAL. Следующая команда создает область данных DTA2 с общими правами доступа *CHANGE:

```
CRTDTAARA DTAARA(ITEMLIB/DTA2) +  
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

В разделе “Присвоение прав доступа и владельца для новых объектов” на стр. 152 приведены дополнительные примеры определения принадлежности и прав доступа при создании объектов.

В параметре библиотеки CRTAUT можно указать имя списка прав доступа. В этом случае все объекты, создаваемые в библиотеке с параметром AUT(*LIBCRTAUT), будут защищены с помощью указанного списка прав доступа. В качестве общих прав доступа к объекту будет установлено значение *AUTL.

Параметр библиотеки CRTAUT не применяется при перемещении (MOV OBJ), создании дубликата (CRTDUPOBJ) и восстановлении объекта библиотеки. В этих случаях применяются общие права доступа существующего объекта.

Если в команде создания задан параметр REPLACE (*YES), то вместо параметра библиотеки CRTAUT применяются права доступа существующего объекта.

Опасность применения прав, устанавливаемых при создании (CRTAUT)

При изменении прав, устанавливаемых при создании (CRTAUT) библиотеки приложений, возникают определенные риски.

Если объектам, создаваемым во время выполнения приложения, присваиваются права доступа по умолчанию, то следует ограничить круг пользователей, которым предоставлены права на изменение описаний библиотек. Изменив значение параметра CRTAUT библиотеки приложения, можно получить несанкционированный доступ к новым объектам библиотеки.

Права доступа к новым объектам каталога

Можно указать права доступа к новым объектам каталога.

При создании каталога с помощью команды CRTDIR, MD или MKDIR (Создать каталог) явно указываются общие права доступа к объекту и данным. Значение по умолчанию, *INDIR, позволяет указать, что для созданного каталога нужно установить те общие права доступа, которые заданы для его родительского каталога. Если права доступа родительского каталога не подходят, можно явно указать необходимые права доступа.

Когда вы создаете каталог с помощью mkdir() - API Создать каталог, права доступа к объекту, присваиваемые владельцу и основной группе, и общие права доступа к объекту определяются по родительскому каталогу, в то время как права доступа к данным, присваиваемые владельцу и основной группе, и общие права доступа к данным определяются по режиму, указанному в вызове API.

В следующих двух примерах иллюстрируется различие результатов создания каталога с разными опциями.

В первом примере каталог создается с помощью команды CRTDIR в корневой (/) файловой системе с заданными правами доступа *PUBLIC.

Начальные условия: права доступа в родительском каталоге:

```

                                Показать права доступа
Объект . . . . . : /sandern/mytest
Владелец . . . . . : SANDERS
Основная группа . . . . . : SANDERSGP3
Список прав доступа . . . . . : *NONE
Права дос. ---Права доступа к объекту--
Пользователь к данным  Суц      Упр      Изм      Обр
*PUBLIC      *RWX      X        X        X        X
SANDERS      *RW
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX      X        X        X        X

```

Пользователь SANDERS вводит следующую команду:

CRDIR DIR(/sandern/mytest/deletemepub) DTAAUT(*R) OBJAUT(*NONE)

Результаты: права доступа в созданном каталоге:

```

                                Показать права доступа
Объект . . . . . : /sandern/mytest/deletemepub
Владелец . . . . . : SANDERS
Основная группа . . . . . : SANDERSGP3
Список прав доступа . . . . . : *NONE
Права дос. ---Права доступа к объекту--
Пользователь к данным  Суц      Упр      Изм      Обр
*PUBLIC      *R
SANDERS      *RWX
SANDERSGP3   *RX

```

Notes:

1. Права доступа к данным и объекту *PUBLIC задаются на основе параметров DTAAUT и OBJAUT.
2. Права доступа к данным владельца (SANDERS) устанавливаются равными *RWX, однако права доступа к объекту наследуются от владельца родительского каталога. Это означает, что у владельца нового каталога нет прав доступа к объекту по отношению к этому каталогу, поскольку у владельца родительского каталога нет прав доступа к объекту по отношению к родительскому каталогу.
3. У нового каталога профайл основной группы равен SANDERSGP3, поскольку этот профайл является основной группой родительского каталога.

Во втором примере демонстрируется, как все права доступа наследуются из родительского каталога, когда каталог создается с помощью команды CRDIR в корневой (/) файловой системе.

Начальные условия: права доступа в родительском каталоге:

```

                                Показать права доступа
Объект . . . . . : /sandern/mytest
Владелец . . . . . : SANDERS
Основная группа . . . . . : SANDERSGP3
Список прав доступа . . . . . : *NONE
Права дос. ---Права доступа к объекту--
Пользователь к данным Суц Упр Изм Обр
*PUBLIC *RWX X X X X
SANDERS *RW
SANDERSGP3 *RX
QPGMR *RWX
QTCM *RWX X X X X
```

Пользователь SANDERSUSR вводит следующую команду:
CRTDIR DIR('/sandern/mytest/deletemepub')

Результаты: права доступа в созданном каталоге:

```

                                Показать права доступа
Объект . . . . . : /sandern/mytest/deletemepub
Владелец . . . . . : SANDERSUSR
Основная группа . . . . . : SANDERSGP3
Список прав доступа . . . . . : *NONE
Права дос. ---Права доступа к объекту--
Пользователь к данным Суц Упр Изм Обр
*PUBLIC *RWX X X X X
SANDERSUSR *RWX
SANDERSGP3 *RX
QPGMR *RWX
QTCM *RWX X X X X
SANDERS *RW
```

Notes:

1. Права доступа к данным и объекту *PUBLIC наследуются от родительского каталога; следовательно, права доступа к данным устанавливаются равными *RWX со всеми правами доступа к объекту.
2. Права доступа к данным владельца (SANDERSUSR) устанавливаются равными *RWX, однако права доступа к объекту наследуются от владельца родительского каталога. Это означает, что у владельца нового каталога нет прав доступа к объекту по отношению к этому каталогу, поскольку у владельца родительского каталога нет прав доступа к объекту по отношению к родительскому каталогу.
3. У нового каталога профайл основной группы равен SANDERSGP3, поскольку этот профайл является основной группой родительского каталога.
4. Всем пользователям, у которых есть частные права доступа к родительскому каталогу (QPGMR, QTCM), и владельцу родительского каталога (SANDERS) предоставляются те же самые частные права доступа к новому каталогу.

Принадлежность объекта

В этом разделе описана принадлежность объектов и ее значение в системе.

Во время создания объекта ему присваивается владелец. Владелец становится тот пользователь, который создал объект, или профайл группы этого пользователя, если в профайле пользователя указано, что владельцем должна быть группа. Владелец предоставляются все права доступа к объекту и данным этого

объекта. В разделе “Присвоение прав доступа и владельца для новых объектов” на стр. 152 приведены примеры определения принадлежности нового объекта.

Владельцу объекта всегда предоставлены все права доступа к объекту, если некоторые из этих прав доступа не были явно аннулированы. В качестве меры предосторожности владелец объекта может удалить некоторые из предоставленных ему прав доступа, если ему не предоставлены специальные права доступа *ALLOBJ. Например, владелец файла, содержащего очень важную информацию, может аннулировать свои права к существованию объекта, для того чтобы случайно не удалить этот файл. Владелец объекта может в любой момент предоставить себе любые права доступа к объекту. У владельца вновь созданного объекта интегрированной файловой системы те же права доступа к объекту по отношению к этому объекту, что и у владельца родительского каталога - по отношению к родительскому каталогу. Информация о том, применяются ли правила о назначении прав доступа к объекту ко всем файловым системам или только к некоторым, приведена в разделе Планирование и настройка защиты системы.

Объект можно передавать от одного владельца к другому. Новым владельцем объекта можно назначить как профайл отдельного пользователя, так и профайл группы. Профайл группы может выступать в роли владельца объекта даже в том случае, если группа не содержит ни одного элемента.

Следующие параграфы относятся к объектам библиотек и каталогов.

При изменении владельца объекта можно аннулировать права доступа предыдущего владельца объекта или сохранить их.

Если профайлу принадлежат какие-либо объекты, то его нельзя удалять. Перед удалением такого профайла необходимо изменить принадлежность его объектов или удалить эти объекты. Команда Удалить пользовательский профайл (DLTUSRPRF) дает возможность обработать принадлежащие профайлу объекты перед его удалением.

Принадлежность объекта применяется системой как один из инструментов управления. Профайл владельца объекта содержит список всех пользователей, которым предоставлены частные права доступа к объекту. Эта информация применяется для создания меню просмотра и редактирования прав доступа к объекту.

Профайлы, которым принадлежит большое число объектов с широким набором частных прав доступа, могут быть очень велики. Размер профайла влияет на производительность работы с правами доступа к объектам, принадлежащим профайлу, а также скорость сохранения и восстановления профайла. Кроме того, он может повлиять на выполнение операций в системе. Во избежание этого не присваивайте одного владельца всем объектам в среде System i5. Каждое приложение вместе со своими объектами должно принадлежать отдельному профайлу. Кроме того, поставляемые фирмой IBM пользовательские профайлы не должны выступать в роли владельцев пользовательских данных или объектов.

Владельцу объекта необходима дополнительная память для хранения информации об этом объекте. Дополнительная информация приведена в разделе “Максимальный объем памяти” на стр. 99.

Групповая принадлежность объектов

В этом разделе описаны особенности принадлежности объектов к группе.

При создании объекта система определяет его владельца исходя из информации, указанной в профайле пользователя, создавшего объект. Если пользователь входит в состав группы, то владельцем объекта назначается сам пользователь или его группа в зависимости от значения параметра OWNER, заданного в профайле пользователя.

Если владельцем объекта назначается группа (параметр OWNER равен *GRPPRF), то создавшему объект пользователю не предоставляются никакие особые права доступа к объекту. Пользователь получает права доступа к объекту посредством группы. Если владельцем объекта назначается пользователь (параметр OWNER равен *USRPRF), то предоставляемые группе права доступа к объекту зависят от значения поля

GRPAUT пользовательского профайла. Объекты, созданные в каталогах, не используют значения OWNER и GRPAUT для определения принадлежности или прав доступа группы. Объект будет всегда принадлежать создателю объекта.

Поле пользовательского профайла *Тип прав доступа группы* (GRPAUTTYP) указывает, становится ли группа основной группой объекта, или же ей предоставляются частные права доступа к объекту. В разделе “Присвоение прав доступа и владельца для новых объектов” на стр. 152 приведено несколько примеров.

В случае изменения группы пользователя, которому принадлежит объект, профайл исходной группы сохраняет права доступа ко всем созданным объектам.

Во время создания объекта у пользователя должно быть достаточно памяти для его хранения, даже если полю *Владелец* в пользовательском профайле присвоено значение *GRPPRF. После создания объекта его владельцем становится профайл группы. Объем вспомогательной памяти, который может быть выделен пользователю, указывается в параметре MAXSTG пользовательского профайла.

При выборе владельца между группой и отдельным пользователем определите, какие объекты (например, программы запросов) пользователь может создать:

- Должен ли пользователь оставаться владельцем объектов после перехода в другой отдел и другую группу пользователей?
- Важно ли знать, кем были созданы объекты? В меню с правами доступа к объекту указывается владелец объекта, а не пользователь, создавший объект.

Примечание: Создавший объект пользователь задан в меню Показать описание объекта.

Если ведется журнал контроля QAUDJRN, то при создании объекта в него заносится запись о создании объекта (CO). В этой записи указывается пользовательский профайл, создавший объект. Такая запись создается только в том случае, если в системном значении QAUDLVL задано значение *CREATE, а в системном значении QAUDCTL указано значение *AUDLVL.

Понятия, связанные с данным

“Профайлы групп” на стр. 5

Профайл группы - это особый тип пользовательского профайла. Если требуется предоставить одинаковые права доступа нескольким пользователям, то с помощью профайла группы вы можете сделать это за один прием.

Основная группа объекта

Для объекта можно задать основную группу.

Имя профайла основной группы и его права доступа к объекту хранятся вместе с объектом. Проверка прав доступа основной группы обычно выполняется быстрее, чем проверка частных прав доступа группы.

В качестве основной группы объекта можно указать только профайл группы (профайл, которому присвоен gid). Один профайл группы нельзя назначить и владельцем объекта, и основной группой объекта.

При создании объекта пользователем система использует информацию из профайла этого пользователя для того чтобы определить, следует ли предоставить группе пользователя права доступа к объекту, и если да, то права какого типа. Группу пользователя можно назначить основной группой объекта с помощью параметра *Тип прав доступа группы* (GRPAUTTYP) пользовательского профайла. В “Присвоение прав доступа и владельца для новых объектов” на стр. 152 описаны примеры присвоения прав доступа при создании объектов. В некоторых файловых системах объекты каталогов наследуют основную группу своих родительских каталогов. Например, если у родительского каталога основная группа - FRED, то FRED не сможет создавать объекты в этом родительском каталоге. Причина этого заключается в том, что один и тот же профайл не может быть одновременно владельцем и профайлом основной группы одного и того же объекта.

Вы можете изменить основную группу объекта библиотеки или каталога с помощью любой из следующих команд:

- Изменить основную группу объекта (CHGOBJPGP)
- Изменить основную группу (CHGPGP)
- Опция 9 команды Работа с объектами по основной группе (WRKOBJPGP)

Права доступа основной группы можно изменить с помощью команды Редактировать права доступа к объекту (EDTOBJAUT) или команд предоставления и аннулирования прав доступа. Права доступа основной группы для объекта библиотеки или каталога можно изменить с помощью команды Изменить права доступа (CHGAUT) или команды Работа с правами доступа (WRKAUT).

Понятия, связанные с данным

“Профайлы групп” на стр. 5

Профайл группы - это особый тип пользовательского профайла. Если требуется предоставить одинаковые права доступа нескольким пользователям, то с помощью профайла группы вы можете сделать это за один прием.

Пользовательский профайл владельца по умолчанию (QDFTOWN)

Пользовательский профайл владельца по умолчанию (QDFTOWN) - это поставляемый фирмой IBM пользовательский профайл, который применяется в тех случаях, когда у объекта нет владельца, а также когда принадлежность объекта может быть использована для обхода защиты.

Профайл QDFTOWN назначается владельцем объекта в следующих случаях:

- Если профайл удаляется из-за повреждения, то принадлежащие ему объекты остаются без владельца. В результате выполнения команды Восстановить память (RCLSTG) владельцем подобных объектов назначается пользовательский профайл владельца по умолчанию (QDFTOWN).
- Если объект был восстановлен, а профайл владельца не существует.
- Если требующая повторного создания программа была восстановлена, однако создать эту программу не удалось. Дополнительная информация о том, при каких условиях владельцем становится профайл QDFTOWN, приведена в разделе “Проверка восстанавливаемых программ” на стр. 18.
- Если превышено ограничение на объем памяти, установленное для пользовательского профайла, которому принадлежит владелец прав доступа с тем же именем, что и у файла, который перемещается или переименовывается, либо библиотеки, которая переименовывается.

Пользовательский профайл QDFTOWN необходим в системе для того, чтобы у всех объектов был владелец. По умолчанию просматривать пользовательский профайл QDFTOWN, обращаться к нему и изменять принадлежность объектов, связанных с этим профайлом, разрешено только пользователю со специальными правами доступа *ALLOBJ. При необходимости доступ к профайлу QDFTOWN можно предоставить и другим пользователям. Пользовательский профайл QDFTOWN предназначен только для внутреннего использования. В обычных случаях профайл QDFTOWN не должен становиться владельцем объектов.

Присвоение прав доступа и владельца для новых объектов

Можно присвоить права доступа и владельца для новых объектов.

Система присваивает права доступа и владельца объекту во время его создания исходя из нескольких значений:

- Параметров команды CRTxxx
- Системного значения QCRTAUT
- Параметра CRTAUT библиотеки
- Параметров профайла пользователя, создавшего объект

В разделах с рис. 6 на стр. 153 по рис. 9 на стр. 156 приведено несколько примеров применения этих значений:

Системное значение QCRTAUT:
*CHANGE

Параметр CRTAUT библиотеки:
*USE

Параметры профайла USERA (профайла пользователя, создающего объект):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Команда создания объекта:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

или

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR)
```

Параметры нового объекта:

Общие права доступа:
*USE

Права доступа владельца:
USERA *ALL

Права доступа основной группы:
Нет

Частные права доступа:
DPT806 *CHANGE

Примечание:

*LIBCRTAUT применяется в качестве значения по умолчанию для параметра AUT в большинстве команд CRTxxx.

Рисунок 6. Пример создания объекта: общие права доступа взяты из параметра библиотеки, группе предоставлены частные права доступа

Системное значение QCRTAUT:
*CHANGE

Параметр CRTAUT библиотеки:
*SYSVAL

Параметры профайла USERA (профайла пользователя, создающего объект):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Команда создания объекта:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Параметры нового объекта:

Общие права доступа:
*CHANGE

Права доступа владельца:
USERA *ALL

Права доступа основной группы:
Нет

Частные права доступа:
DPT806 *CHANGE

Рисунок 7. Пример создания объекта: общие права доступа взяты из системного значения, группе предоставлены частные права доступа

Системное значение QCRTAUT:
*CHANGE

Параметр CRTAUT библиотеки:
*USE

Параметры профайла USERA (профайла пользователя, создающего объект):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PGP

Команда создания объекта:
CRTDTAARA DTAARA(CUSTLIB/DTA1)
TYPE(*CHAR) AUT(*LIBCRTAUT)

Параметры нового объекта:

Общие права доступа:
*USE

Права доступа владельца:
USERA *ALL

Права доступа основной группы:
DPT806 *CHANGE

Частные права доступа:
Нет

Рисунок 8. Пример создания объекта: общие права доступа взяты из параметра библиотеки, группе предоставлены права доступа основной группы

Системное значение QCRTAUT:

*CHANGE

Параметр CRTAUT библиотеки:

*USE

Параметры профайла USERA (профайла пользователя, создающего объект):

GRPPRF:

DPT806

OWNER:

*GRPPRF

GRPAUT:

GRPAUTTYP:

Команда создания объекта:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR) AUT(*CHANGE)
```

Параметры нового объекта:

Общие права доступа:

*CHANGE

Права доступа владельца:

DPT806 *ALL

Права доступа основной группы:

Нет

Частные права доступа:

Нет

Рисунок 9. Пример создания объекта: предоставлены общие права доступа, группа владеет объектом

Объекты, принимающие права доступа владельца

Пользовательской программе можно предоставить принятые права доступа, чтобы разрешить ей изменение нужного файла.

Иногда пользователю требуются различные права доступа к объекту или приложению в зависимости от ситуации. Например, пользователю может быть разрешено изменять информацию в файле заказчиков с помощью прикладных программ, предоставляющих соответствующую функцию. В то же время, ему может быть разрешено просматривать, но не изменять информацию о заказчиках в средстве поддержки принятия решений, таком как SQL.

В этом случае следует выполнить следующие действия: 1) предоставить пользователю права доступа *USE к информации о заказчиках, для того чтобы пользователь мог запрашивать данные из файлов; 2) использовать принятые права доступа в программах обслуживания заказчиков, для того чтобы пользователь мог изменять файлы.

Когда объект использует права доступа владельца, то говорят, что он *принял права доступа*. Права доступа могут принимать объекты типа *PGM, *SRVPGM, *SQLPKG, а также программы на Java.

В команде CRTxxxPGM, предназначенной для создания программы, предусмотрен параметр пользовательского профайла (USRPRF). Этот параметр указывает, будет ли программа применять права доступа своего владельца в дополнение к правам доступа пользователя, запустившего программу.

Информация об обеспечении защиты и применении принятых прав доступа при работе с пакетами SQL приведена в разделе Ограничение применения принятых прав доступа.

Обратите внимание на следующие свойства принятых прав доступа:

- Принятые права доступа добавляются к существующим правам доступа пользователя.
- Принятые права доступа проверяются только в том случае, если права доступа пользователя, права доступа группы и общие права доступа к объекту недостаточны для выполнения запрошенной операции.
- Специальные права доступа из профайла владельца (такие как *ALLOBJ) применяются наряду с обычными правами доступа.
- Если профайл владельца является элементом группы, то права доступа этой группы *не* включаются в состав принятых прав доступа.
- Общие права доступа *не* включаются в состав принятых прав доступа. Для примера предположим, что пользователь USER1 запустил программу LSTCUST, которой требуются права доступа *USE к файлу CUSTMST:
 - Общие права доступа к файлу CUSTMST равны *USE.
 - Права доступа USER1 равны *EXCLUDE.
 - Программа LSTCUST принимает права доступа своего владельца (пользователя USER2).
 - USER2 не является владельцем файла CUSTMST. У него нет частных прав доступа к этому файлу.
 - В описанном случае пользователю USER1 не будет предоставлен доступ к файлу, хотя общих прав доступа достаточно для того, чтобы пользователь USER2 получил доступ к файлу. Это связано с тем, что принятые права доступа включают в себя только права доступа владельца, права доступа основной группы и частные права доступа.
 - Принимаются только права доступа. Никакие другие атрибуты пользовательского профайла не принимаются. Например, атрибуты ограниченных возможностей не принимаются.
- Принятые права доступа применяются в течение всего времени, пока программа, принявшая права доступа, остается в стеке вызова. Для примера предположим, что программа PGMA использует принятые права доступа:
 - Если PGMA запускает PGMB с помощью команды CALL, то стек вызова до и после вызова команды CALL будет выглядеть следующим образом:

Таблица 119. Принятые права доступа и команда CALL

Стек до вызова команды CALL:	Стек после вызова команды CALL:
QCMD	QCMD
•	•
•	•
•	•
PGMA	PGMA
	PGMB

Поскольку PGMA остается в стеке после вызова PGMB, PGMB будет применять принятые права доступа программы PGMA. (Это можно переопределить с помощью параметра (USEADPAUT). За дополнительной информацией об этом параметре обратитесь к разделу “Программы, игнорирующие принятые права доступа” на стр. 160.)

- Если программа PGMA запускает PGMB с помощью команды Передать управление (TFRCTL), то стек будет выглядеть следующим образом:

Таблица 120. Принятые права доступа и команда TFRCTL

Стек до вызова команды TFRCTL:	Стек после вызова команды TFRCTL:
QCMD	QCMD
•	•
•	•
•	•
PGMA	PGMB

PGMB не будет применять принятые права доступа программы PGMA, так как PGMA больше не находится в стеке вызовов.

- Если выполнение программы, использующей принятые права доступа, будет прервано, то применение этих прав доступа будет приостановлено. Следующие функции не применяют принятые права доступа:
 - Системный запрос
 - Клавиша Attention (в случае вызова команды Перейти к групповому заданию (TFRGRPJOB) принятые права доступа не передаются групповому заданию.)
 - Программа обработки прерывающих сообщений
 - Функции отладки

Примечание: При нажатии клавиши Attention или отправке запроса к групповому заданию применение принятых прав доступа немедленно прерывается. Для успешного выполнения операции пользователю должны быть предоставлены права на выполнение к программе обработки нажатия клавиши Attention или начальной программе группового задания.

Для примера предположим, что пользователь USERA запустил программу PGM1, принимающую права доступа пользователя USERB. Программа PGM1 вызвала команду SETATNPGM, указав программу PGM2. Пользователю USERB предоставлены права доступа *USE к PGM2. Пользователю USERA предоставлены права доступа *EXCLUDE к PGM2. Функция SETATNPGM будет успешно выполнена, так как она использует принятые права доступа. Однако при нажатии клавиши Attention пользователь USERA получит сообщение об ошибке прав доступа, так как в этот момент права доступа пользователя USERB не будут действовать.

- Если принявшая права доступа программа запустит задание, то этому заданию не будут предоставлены принятые права доступа программы.
- При вызове программы триггера или программы выхода ей не предоставляются принятые права доступа предыдущих программ из стека вызова.
- Принятые права доступа не используются в интегрированных файловых системах, включая корневую (/), QOpenSys, QDLS и пользовательские файловые системы.
- Принятые права доступа не применяются при изменении очереди вывода задания с помощью команды Изменить задание (CHGJOB). Для успешного выполнения операции у пользователя, отправившего запрос на изменение, должны быть права доступа к новой очереди вывода.
- Владельцем всех создаваемых программой объектов, в том числе буферных файлов, которые могут содержать конфиденциальную информацию, становится пользователь программы или его группа, а не владелец программы.
- Принятые права доступа можно задать в команде создания программы (CRTxxxPGM) или в команде Изменить программу (CHGPGM) или Изменить служебную программу (CHGSRVPGM).
- Если для создания программы применяется команда CRTxxxPGM с параметром REPLACE(*YES), то новая копия программы сохраняет те значения параметров USRPRF, USEADPAUT и AUT, которые были присвоены заменяемой программе. При этом значения параметров USRPRF и AUT, указанные в команде CRTxxxPGM, игнорируются.
- Если для исходной программы задан параметр USRPRF(*OWNER), то команду CRTxxxPGM с параметром REPLACE(*YES) может вызывать только владелец программы.
- Значение параметра USRPRF разрешено изменять только владельцу программы и пользователям со специальными правами доступа *ALLOBJ и *SECADM.

- Изменять принадлежность объекта, использующего принятые права доступа, может только пользователь со специальными правами доступа *ALLOBJ и *SECADM.
- Если программу, принимающую права доступа, восстановит пользователь, отличный от владельца программы и не имеющий специальных прав доступа *ALLOBJ и *SECADM, то по соображениям защиты все частные и общие права доступа к программе будут аннулированы.

С помощью команд Показать программу (DSPPGM) и Показать служебную программу (DSPSRVPGM) можно узнать, принимает ли программа права доступа (поле *Пользовательский профайл*) и использует ли она принятые права доступа предыдущих программ из стека вызовов (поле *Использует принятые права доступа*). Команда Показать принимающие программы (DSPPGMADP) показывает список всех объектов, принимающих права доступа указанного пользовательского профайла. Команда Печатать принимающие объекты (PRTADPOBJ) создает отчет с более подробной информацией об объектах, принимающих права доступа. Кроме того, в этой команде предусмотрена опция печати отчета об объектах, которые были изменены с момента предыдущего вызова команды.

Дополнительная информация о принятых правах доступа приведена в разделе “Блок-схема 8: Проверка принятых прав доступа” на стр. 191. Пример применения принятых прав доступа в приложении приведен в разделе “Применение принятых прав доступа при разработке меню” на стр. 242.

Принятые права доступа и связанные программы:

Программа ILE* (*PGM) состоит из одного или нескольких модулей. Она создается компилятором ILE*. Программа ILE может быть связана с одной или несколькими служебными программами (*SRVPGM).

Для успешной активации программы ILE пользователю должны быть предоставлены права доступа *EXECUTE к самой программе ILE и всем служебным программам, с которыми она связана. Если программа ILE использует принятые права доступа программы, которая расположена выше нее в стеке вызовов, то эти права доступа применяются для проверки прав доступа к связанным служебным программам. Если программа ILE сама принимает права доступа, эти права доступа не применяются для проверки прав доступа пользователя к служебным программам во время активации.

Принятые права доступа: риски и рекомендации

Применять принятые права доступа следует с осторожностью во избежание нарушения защиты.

Позволяя программе использовать принятые права доступа, вы намеренно ослабляете контроль. Пользователю предоставляется возможность получить дополнительные права доступа к объектам, а в некоторых случаях - и специальные права доступа, которых у него обычно нет. Принятые права доступа дают возможность предоставлять различные права доступа в зависимости от ситуации, однако при работе с ними следует соблюдать следующие меры предосторожности:

- Приложение должно принимать минимальные права доступа, необходимые для выполнения его функций. Лучше, если приложение будет принимать права доступа своего владельца, а не права доступа пользователя QSECOFR или пользователя со специальными правами доступа *ALLOBJ.
- Тщательно отслеживайте набор функций, который предоставляется программами, принимающими права доступа. Убедитесь, что эти программы не дают пользователю возможность работать с объектами, которые не требуются непосредственно для выполнения программы, в частности со средством ввода команд.
- Если программа использует принятые права доступа, то при вызове других программ она должна явно указывать имя библиотеки. При вызове программ не следует использовать список библиотек (*LIBL).
- Ограничьте доступ к программам, использующим принятые права доступа. Это можно сделать с помощью интерфейсов меню и защиты библиотек.

Программы, игнорирующие принятые права доступа

Указать, будет ли программа использовать принятые права доступа, можно с помощью параметра (USEADPAUT).

В некоторых случаях требуется запретить программе использовать принятые права доступа предыдущих программ из стека вызовов. Например, если программа начального меню принимает права доступа своего владельца, то может быть нежелательно, чтобы вызванные из начального меню программы использовали принятые права доступа.

Параметр программы Применять принятые права доступа (USEADPAUT) позволяет указать, следует ли использовать принятые права доступа предыдущих программ из стека вызовов при проверке прав доступа к объектам.

При создании программы по умолчанию разрешается использовать принятые права доступа предыдущих программ из стека вызовов. Если программа не должна применять принятые права доступа, то необходимо изменить значение параметра USEADPAUT на *NO с помощью команды Изменить программу (CHGPGM) или Изменить служебную программу (CHGSRVPGM). Если для создания программы применяется команда CRTxxxPGM с параметром REPLACE(*YES), то новая копия программы сохраняет те значения параметров USRPRF, USEADPAUT и AUT, которые были присвоены заменяемой программе.

Пример применения этого параметра при создании меню приведен в разделе “Игнорирование принятых прав доступа” на стр. 245. Информация о системном значении QUSEADPAUT приведена в разделе “Применять принятые права доступа (QUSEADPAUT)” на стр. 38.

Внимание: В некоторых случаях можно предотвратить передачу принятых прав доступа вызванной функции с помощью инструкции машинного интерфейса MODINVAU. Инструкция MODINVAU позволяет запретить передачу принятых прав доступа от программы на С или С++ вызванной функции другой программы или служебной программы. Эта инструкция может применяться в тех случаях, когда значение параметра USEADPAUT вызываемой функции неизвестно.

Понятия, связанные с данным

“Игнорирование принятых прав доступа” на стр. 245

При применении принятых прав доступа в проектировании меню пользователю необходимо перейти в начальное меню. Для того чтобы пользователи могли запускать запросы как с помощью начального меню, так и с помощью меню приложений, настройте программу QRYSTART для игнорирования принятых прав доступа.

Владельцы прав доступа

Владелец прав доступа - это объект, хранящий права доступа к описанному в программе файлу базы данных, которого в настоящее время нет в системе.

Такие объекты, как владельцы прав доступа, главным образом применяются в приложениях System/36, которые часто удаляют и заново создают описанные в программе файлы.

Владельца прав доступа можно создать для существующего или несуществующего файла с помощью команды Создать владельца прав доступа (CRTAUTHLR). Обратите внимание на следующие свойства владельцев прав доступа:

- Владелец прав доступа можно создавать только для файлов из системного ASP и базовых пользовательских ASP. Их нельзя создавать для файлов из независимых ASP.
- Владелец прав доступа связан с конкретным файлом или библиотекой. Его имя совпадает с именем связанного файла.
- Владельцы прав доступа могут применяться только для программно описанных файлов баз данных и логических файлов.

- После создания владельца прав доступа для него можно установить частные права доступа так же, как и для обычного файла. При вызове команд предоставления, аннулирования или просмотра прав доступа для владельца прав доступа следует указывать тип объекта *FILE. В меню прав доступа к объектам владелец прав доступа ничем не отличается от связанного с ним файла. В этих меню не указывается, существует ли файл и создан ли для него владелец прав доступа.
- Если файл связан с владельцем прав доступа, то при проверке прав доступа применяются те права доступа, которые определены для владельца объекта. Все частные права доступа к файлу игнорируются.
- С помощью команды Показать владельца прав доступа (DSPAUTHLR) можно просмотреть и напечатать полный список владельцев прав доступа, созданных в системе. Кроме того, эта команда позволяет создать файл вывода (OUTFILE) для последующей обработки.
- При создании владельца прав доступа для существующего файла следует обратить внимание на следующее:
 - Для создания владельца прав доступа необходимы права доступа *ALL к файлу.
 - Владелец прав доступа всегда принадлежит тому профайлу, которому принадлежит связанный с ним файл, а не тому пользователю, который создал владельца прав доступа.
 - Владелец прав доступа наследует общие права доступа от связанного с ним файла. Значение, указанное в параметре общих прав доступа (AUT) команды CRTAUTHLR, игнорируется.
 - Права доступа к существующему файлу копируются в объект владельца прав доступа.
- При создании файла, для которого ранее был создан владелец прав доступа, следует учитывать следующее:
 - Для создания файла необходимы права доступа *ALL к владельцу прав доступа.
 - Файл всегда принадлежит тому профайлу, которому принадлежит владелец прав доступа, а не пользователю, создавшему файл.
 - Файл наследует общие права доступа от владельца прав доступа. Значение, указанное в параметре общих прав доступа (AUT) команды CRTPF или CRTLF, игнорируется.
 - Владелец прав доступа подключается к созданному файлу. Для защиты файла применяются права доступа, заданные для владельца прав доступа.
- В случае удаления владельца прав доступа вся информация о правах доступа передается самому файлу.
- Если файлу будет присвоено новое имя, совпадающее с именем существующего владельца прав доступа, то права доступа и владелец файла будут изменены в соответствии с атрибутами владельца прав доступа. Для переименования файла пользователю должны быть предоставлены права доступа *ALL к владельцу прав доступа.
- Если файл будет перемещен в другую библиотеку, и в системе будет обнаружен владелец прав доступа для имени этого файла и целевой библиотеки, то права доступа и владелец файла будут изменены в соответствии с атрибутами владельца прав доступа. Для перемещения файла пользователю должны быть предоставлены права доступа *ALL к владельцу прав доступа.
- Принадлежность владельца прав доступа всегда совпадает с принадлежностью файла. При изменении принадлежности файла изменяется и принадлежность владельца прав доступа.
- Если после восстановления файла в системе будет найден владелец прав доступа для файла с таким именем, расположенного в целевой библиотеке, то этот владелец будет подключен к файлу.
- Владелец прав доступа нельзя создавать для файлов из следующих библиотек: QSYS, QRCL, QRECOVERY, QSPL, QTEMP и QSPL0002 – QSPL0032.

Владельцы прав доступа и перенос данных System/36

Средство переноса данных System/36 создает владельца прав доступа для каждого перенесенного файла. Кроме того, оно создает владельца прав доступа для записей файла защиты ресурсов System/36, если аналогичного файла нет в системе System/36.

Владельцы прав доступа необходимы только для тех файлов, которые удаляются и заново создаются в приложениях. Ненужные владельцы прав доступа можно удалить с помощью команды Удалить владельца прав доступа (DLTAUTHLR).

Риски при работе с владельцами прав доступа

При работе с владельцами прав доступа необходимо знать связанные с этим риски.

Владелец прав доступа дает возможность определить права доступа к файлу до создания этого файла. При соблюдении ряда условий это позволяет злоумышленнику получить доступ к информации. Если пользователь заранее знает, что приложение создает, перемещает или переименовывает некоторый файл, то он может создать владельца прав доступа для нового файла. Таким образом пользователь получает доступ к файлу.

Для того чтобы исключить возникновение подобных ситуаций, команда CRTAUTHLR поставляется с общими правами доступа *EXCLUDE. Это означает, что данную команду смогут применять только пользователи с правами доступа *ALLOBJ, если вы не предоставите права доступа к команде другим пользователям.

Работа с правами доступа

В этом разделе описаны стандартные способы настройки, обслуживания и просмотра прав доступа в системе.

Полный список команд, предназначенных для работы с правами доступа, можно найти в разделе Приложение А, “Команды для организации защиты”, на стр. 327. В приведенных описаниях указана информация не о всех параметрах команды и полях меню. Полную информацию можно найти в электронной справке.

Меню прав доступа

В этом разделе приведено краткое описание меню, показывающих права доступа к объекту.

Права доступа к объекту можно просмотреть с помощью четырех меню:

- Показать права доступа к объекту
- Редактировать права доступа к объекту
- Показать права доступа
- Работа с правами доступа

На рис. 10 показано основное представление меню Показать права доступа к объекту.

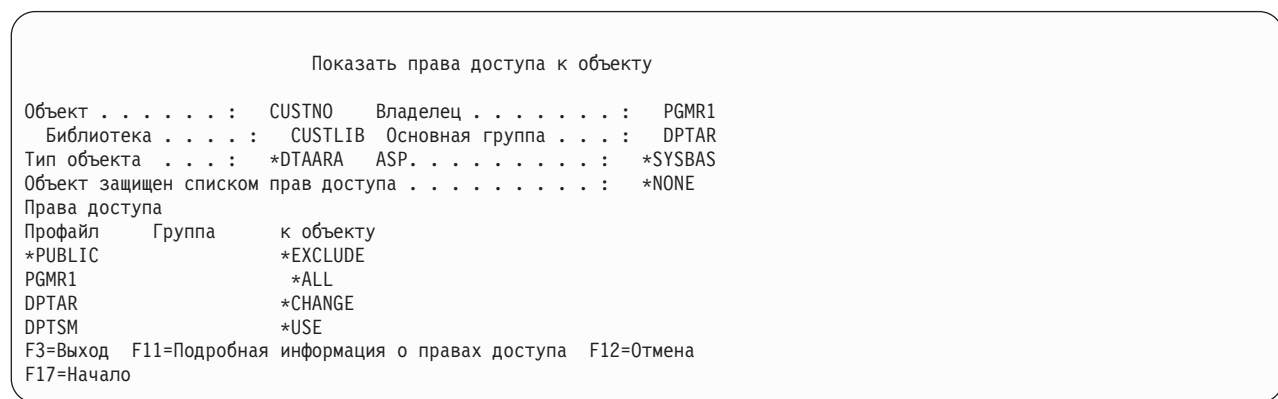


Рисунок 10. Показать права доступа к объекту

В этом меню показаны системные имена прав доступа. Клавиша F11 служит переключателем между основным представлением и двумя другими представлениями меню. Одно из них содержит подробную информацию о правах доступа к объекту:


```

Показать права доступа к объекту
Объект . . . . . : CUSTNO Владелец . . . . . : PGMRI
Библиотека . . . . : CUSTLIB Основная группа . . . : DPTAR
Тип объекта. . . . : *DTAARA ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа. . . . . : *NONE
Права к -----Объект-----
Пользоват  Группа  объекту  Опрц Упр  Суц  Изменен Обр
*PUBLIC    *EXCLUDE  X
PGMR1      *ALL      X  X  X  X  X
DPTAR      *CHANGE   X
DPTSM      *USE      X
:
:
F3=Выход F11=Права доступа к данным F12=Отмена F17=Начало F18=Конец

```

В другом представлении показаны права доступа к данным:

```

Показать права доступа к объекту
Объект . . . . . : CUSTNO Владелец . . . . . : PGMRI
Библиотека . . . . : CUSTLIB Основная группа . . . : DPTAR
Тип объекта. . . . : *DTAARA ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : *NONE
Права -----Данные-----
Пользоват  Группа  к объекту  Чтение Добав Обнов Удаление Выполнен
*PUBLIC    *EXCLUDE
PGMR1      *ALL      X  X  X  X  X
DPTAR      *CHANGE   X  X  X  X  X
DPTSM      *USE      X  X  X  X  X

```

Если вам предоставлены права доступа *OBJMGT к объекту, то вы можете просмотреть все частные права доступа к этому объекту. Если права доступа *OBJMGT не предоставлены, то вы можете просмотреть только свои источники прав доступа к объекту.

Например, если пользователь USERA просматривает права доступа к области данных CUSTNO, то будут показаны только общие права доступа.

Если пользователь USERB, входящий в состав группы DPTAR, попытается просмотреть права доступа к области данных CUSTNO, то будет показано следующее меню:

```

Показать права доступа к объекту
Объект . . . . . : CUSTNO Владелец . . . . . : PGMRI
Библиотека . . . . : CUSTLIB Основная группа . . . : DPTAR
Тип объекта. . . . : *DTAARA ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : *NONE
Права доступа
Профайл  Группа  к объекту
*GROUP   DPTAR  *CHANGE

```

Если пользователь USERB запустит программу, принимающую права доступа PGMRI, и попытается просмотреть права доступа к области данных CUSTNO, то будет показано следующее меню:

Показать права доступа к объекту

```

Объект . . . . . : CUSTNO   Владелец . . . . . : PGMRI
Библиотека . . . : CUSTLIB  Основная группа . . . : DPTAR
Тип объекта. . . : *DTAARA  ASP. . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : *NONE
    
```

Профайл	Группа	Права доступа к объекту
*ADOPTED		USER DEF
*PUBLIC		*EXCLUDE
PGMR1		*ALL
*GROUP	DPTAR	*CHANGE
DPTSM		*USE

Права доступа *ADOPTED представляют только дополнительные права доступа, полученные от владельца программы. Пользователь USERB получил от PGMRI все права доступа, не входящие в состав группы прав доступа *CHANGE. В меню показаны все частные права доступа, так как пользователь USERB принял права доступа *OBJMGT. Меню с подробной информацией будет выглядеть следующим образом:

Показать права доступа к объекту

```

Объект . . . . . : CUSTNO   Владелец . . . . . : PGMRI
Библиотека . . . : CUSTLIB  Основная группа . . . : DPTAR
Тип объекта. . . : *DTAARA  ASP. . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : *NONE
    
```

Пользоват	Группа	Права к объекту	-----Объект-----				
			Опрц	Упр	Сущ	Изменен	Обр
*ADOPTED		USER DEF		X	X	X	X
*PUBLIC		*EXCLUDE					
PGMR1		*ALL	X	X	X	X	X
*GROUP	DPTAR	*CHANGE	X				
DPTSM		*USE	X				

F3=Выход F11=Права доступа к данным F12=Отмена F17=Начало F18=Конец

Если в поле опции пользователя (USROPT) пользовательского профайла USERB указано значение *EXPERT, то меню будет выглядеть следующим образом:

Показать права доступа к объекту

```

Объект . . . . . : CUSTNO   Владелец . . . . . : PGMRI
Библиотека . . . : CUSTLIB  Основная группа . . . : DPTAR
Тип объекта. . . : *DTAARA  ASP. . . . . : *SYSBAS
Объект защищен списком прав доступа. . . . . : *NONE
    
```

Польз	Группа	Права к объекту	----Объект----					-----Данные-----				
			O	M	E	A	R	R	A	U	D	E
*ADOPTED		USER DEF			X	X			X	X		
*PUBLIC		*EXCLUDE										
PGMR1		*ALL	X	X	X	X	X	X	X	X	X	
*GROUP	DPTAR	*CHANGE	X					X	X	X	X	
DPTSM		*USE	X					X			X	

Отчеты о правах доступа

Для контроля за текущей реализацией схемы защиты можно создавать различные отчеты.

Например, для получения информации об объектах, права доступа *PUBLIC к которым отличны от *EXCLUDE, и объектах с частными правами доступа можно воспользоваться следующими командами:

- Печатать общие права доступа (PRT PUBAUT)

- Печатать частные права доступа (PRTPVTAUT)

Информация, связанная с данной

Инструменты защиты системы

Работа с библиотеками

Можно указать права доступа к библиотекам и новым объектам библиотеки.

На права доступа влияют два параметра команды Создать библиотеку (CRTLIB):

Права доступа (AUT): С помощью параметра AUT можно задать одно из следующих значений:

- Общие права доступа к библиотеке
- Список прав доступа, применяемый для защиты библиотеки.

Параметр AUT относится к самой библиотеке, а не к содержащимся в ней объектам. Если в параметре будет задано имя списка прав доступа, то для библиотеки будут установлены общие права доступа *AUTL.

Если при создании библиотеки не будет задан параметр AUT, то по умолчанию будет установлено значение *LIBCRTAUT. Это означает, что будет применяться значение параметра CRTAUT библиотеки QSYS, которое первоначально равно *SYSVAL.

Права при создании (CRTAUT): Параметр CRTAUT задает права доступа, которые по умолчанию устанавливаются для всех объектов, создаваемых в библиотеке. Параметру CRTAUT можно присвоить одно из системных значений прав доступа (*ALL, *CHANGE, *USE или *EXCLUDE), значение *SYSVAL (системное значение QCRTAUT) или имя списка прав доступа.

Примечание: Параметр библиотеки CRTAUT можно изменить с помощью команды Изменить библиотеку (CHGLIB).

Если пользователь PGMRI введет следующую команду:

```
CRTLIB TESTLIB AUT(LIBLST) CRTAUT(OBJLST)
```

то права доступа к библиотеке будут выглядеть следующим образом:

```

Показать права доступа к объекту
Объект . . . . . : TESTLIB      Владелец . . . . . : PGMRI
Библиотека . . . . : QSYS        Основная группа . . . : *NONE
Тип объекта . . . . : *LIB        ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. : LIBLST

Профайл      Группа      Права доступа
*PUBLIC      *ALL        к объекту
PGMRI
*AUTL

```

- Поскольку в параметре AUT был задан список прав доступа, общие права доступа равны *AUTL.
- Запустивший команду CRTLIB пользователь становится владельцем новой библиотеки, если в его профайле не указано OWNER(*GRPPRF). Владельцу автоматически предоставляются права доступа *ALL.
- Значение параметра CRTAUT не указывается в меню прав доступа к объекту. Его можно просмотреть с помощью команды Показать описание библиотеки (DSPLIBD).

Показать описание библиотеки

```
Library . . . . . : TESTLIB
Тип . . . . . : PROD
Номер ASP . . . . . : 1
ASP . . . . . : *SYSBAS
Права при создании . . . . . : OBJLST
Контроль за объектом при создании . . . . . : *SYSVAL
Описание . . . . . : Customer Rec
```

Создание объектов

При создании нового объекта ему присваиваются настроенные права доступа.

При создании объекта можно явно указать права доступа в параметре AUT или воспользоваться значением по умолчанию, *LIBCRTAUT. Если пользователь PGMR1 введет следующую команду:

```
CRTDTAARA (TESTLIB/DTA1) +
  TYPE(*CHAR)
```

то права доступа к области данных будут выглядеть следующим образом:

Показать права доступа к объекту

```
Объект . . . . . : DTA1      Владелец . . . . . : PGMR1
Библиотека . . . . . : TESTLIB  Основная группа . . . . . : *NONE
Тип объекта . . . . . : *DTAARA  ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : OBJLST

Профайл      Группа      Права доступа
*PUBLIC      *ALL      к объекту
PGMR1      *ALL      *AUTL
```

Список прав доступа (OBJLST) взят из параметра CRTAUT, указанного при создании библиотеки TESTLIB.

Если пользователь PGMR1 введет следующую команду:

```
CRTDTAARA (TESTLIB/DTA2) AUT(*CHANGE) +
  TYPE(*CHAR)
```

то права доступа к области данных будут выглядеть следующим образом:

Показать права доступа к объекту

```
Объект . . . . . : DTA2      Владелец . . . . . : PGMR1
Библиотека . . . . . : TESTLIB  Основная группа . . . . . : *NONE
Тип объекта . . . . . : *DTAARA  ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : *NONE

Профайл      Группа      Права доступа
*PUBLIC      *ALL      к объекту
PGMR1      *ALL      *CHANGE
```

Работа с правами доступа к отдельным объектам

В этом разделе описано изменение прав доступа к объекту.

Для изменения прав доступа к объекту должно быть выполнено одно из следующих условий:

- Вам предоставлены права доступа *ALLOBJ, либо вы входите в состав группы, которой предоставлены такие права доступа.

Примечание: Права доступа группы не применяются, если вам предоставлены частные права доступа к объекту.

- Вы являетесь владельцем объекта. Если владельцем является профайл группы, то любой элемент этой группы может действовать как владелец объекта при условии, что этому элементу не предоставлены права доступа, не позволяющие изменять права доступа к объекту.
- Вам предоставлены права доступа *OBJMGT к объекту и все предоставляемые или аннулируемые права доступа (за исключением *EXCLUDE). Предоставлять и аннулировать права доступа *EXCLUDE может любой пользователь, которому разрешено работать с правами доступа к объекту.

Права доступа к отдельному объекту проще всего изменить с помощью меню Редактировать права доступа к объекту. Для того чтобы открыть это меню, нужно вызвать команду Редактировать права доступа к объекту (EDTOBJAUT) или выбрать соответствующую опцию в меню Работа с объектами по владельцу, Работа с объектами по частным правам доступа, Работа с объектами по основной группе или Работа с объектами.

```

                                Редактировать права доступа к объекту
Объект . . . . . : DTA1      Владелец . . . . . : PGMR1
Библиотека . . . : TESTLIB  Основная группа . . . : *NONE
Тип объекта. . . : *DTAARA  ASP. . . . . : *SYSBAS
Измените текущие права доступа и нажмите Enter.

    Объект защищен списком прав доступа . . . . . : OBJLST
Права доступа
Профайл      Группа      к объекту
*PUBLIC      *AUTL
PGMR1        *ALL
```

Права доступа к объекту можно изменить и с помощью следующих команд:

- Изменить права доступа (CHGAUT)
- Работа с правами доступа (WRKAUT)
- Предоставить права доступа к объекту (GRTOBJAUT)
- Аннулировать права доступа к объекту (RVKOBJAUT)

Для предоставления стандартных наборов прав доступа, таких как права на чтение и запись (*RX) или права на запись и выполнение (*WX), необходимо использовать команду CHGAUT или WRKAUT.

Настройка пользовательских прав доступа

Этот раздел содержит информацию о настройке пользовательских прав доступа.

В поле Права доступа к объекту меню Редактировать права доступа к объекту можно указать любой системный набор прав доступа (*ALL, *CHANGE, *USE, *EXCLUDE). Для того чтобы задать другой набор прав доступа нужно нажать клавишу F11 (Показать сведения).

Примечание: Если в поле пользовательского профайла Опции пользователя (USROPT) задано значение *EXPERT, то пользователь всегда будет видеть подробное представление меню. Для просмотра такого представления ему не требуется нажимать F11.

Предположим, что пользователь PGMR1 удалил права доступа *OBJEXIST к файлу CONTRACTS, чтобы предотвратить случайное удаление этого файла. Поскольку сочетание прав доступа PGMR1 не совпадает ни с одним из системных наборов прав доступа, то в столбце Права к объекту для этого пользователя будет указано значение *USER DEF* (пользовательские права доступа):

```

                                Редактировать права доступа к объекту
Объект . . . . . : CONTRACTS  Владелец . . . . . : PGMR1
Библиотека . . . . : TESTLIB   Основная группа . . . : *NONE
Тип объекта. . . . : *FILE     ASP. . . . . : *SYSBAS
Измените текущие права доступа и нажмите Enter.

    Объект защищен списком прав доступа . . . . . : LIST2

Пользоват  Группа      Права к -----Объект-----
*PUBLIC    *AUTL
PGMR1      USER DEF   X   X               X   X
  
```

Для просмотра или изменения прав доступа к данным нажмите F11 (Права доступа к данным):

```

                                Редактировать права доступа к объекту
Объект . . . . . : CONTRACTS  Владелец . . . . . : PGMR1
Библиотека . . . . : TESTLIB   Основная группа . . . : *NONE
Тип объекта. . . . : *FIL      ASP. . . . . : *SYSBAS
Измените текущие права доступа и нажмите Enter.

    Объект защищен списком прав доступа . . . . . : LIST2

Пользоват  Группа      Права -----Данные-----
к объекту  Чтение Добав Обнов Удаление Выполнен
*PUBLIC    *AUTL
PGMR1      USER DEF   X   X   X       X       X
  
```

Предоставление прав доступа новым пользователям

В этом разделе описано предоставление прав доступа новым пользователям.

Для того чтобы предоставить права доступа новым пользователям, нажмите F6 (Добавить пользователей) в меню Редактировать права доступа к объекту. Появится меню Добавить пользователей, позволяющее определить права доступа для нескольких пользователей:

```

                                Добавить пользователей

Объект . . . . . : DTA1
Библиотека . . . . : TESTLIB

Укажите новых пользователей, нажмите Enter.

Пользоват  Права доступа
к объекту
USER1      *USE
USER2      *CHANGE
PGMR2      *ALL
  
```

Аннулирование прав доступа пользователя

Права доступа пользователя к объекту можно аннулировать.

Аннулирование прав доступа пользователя к объекту отличается от предоставления пользователю прав доступа *EXCLUDE. Наличие прав доступа *EXCLUDE означает, что пользователю явно запрещен доступ к объекту. Такие права доступа переопределяются только специальными правами доступа *ALLOBJ и принятыми правами доступа.

Примечание: Права доступа *EXCLUDE к профайлу группы можно переопределить, если у пользователя есть другой профайл группы с частными правами доступа к объекту.

Аннулирование прав доступа пользователя означает, что пользователю не предоставлены никакие особые права доступа к объекту. При этом пользователь может получить доступ к объекту через профайл группы, список прав доступа, общие права доступа, специальные права доступа *ALLOBJ или принятые права доступа.

Права доступа пользователя можно аннулировать с помощью меню Редактировать права доступа к объекту. Для этого введите пробелы в поле Права к объекту напротив имени пользователя и нажмите клавишу Enter. Имя пользователя больше не будет показано в меню. Кроме того, права доступа можно удалить с помощью команды Аннулировать права доступа к объекту (RVKOBJAUT). Она позволяет аннулировать отдельные права доступа пользователя или права доступа *ALL.

Примечание: Команда RVKOBJAUT аннулирует только указанные права доступа. Для примера предположим, что пользователю USERB предоставлены права доступа *ALL к файлу FILEB из библиотеки LIBB. В этом случае можно аннулировать только права доступа *CHANGE:

```
RVKOBJAUT OBJ(LIBB/FILEB) OBJTYPE(*FILE) +
USER(*USERB) AUT(*CHANGE)
```

После выполнения этой команды пользователю USERB будут предоставлены следующие права доступа к файлу FILEB:

```

Показать права доступа к объекту
Объект . . . . . : FILEB      Владелец . . . . . : PGMRI
Библиотека . . . . : LIBB      Основная группа . . : *NONE
Тип объекта . . . . : *FILE    ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . : *NONE
Права к -----Объект-----
Пользоват  Группа  объекту  Опрц Упр  Суц  Изменен Обр
USERB      USER DEF      X   X      X   X

```

```

Показать права доступа к объекту
Объект . . . . . : FILEB      Владелец . . . . . : PGMRI
Библиотека . . . . : LIBB      Основная группа . . : *NONE
Тип объекта . . . . : *FILE    ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . . :
*NONE
Права -----Данные-----
Пользоват  Группа  к объекту  Чтение Добав Обнов Удаление Выполнен
USERB      USER DEF

```

Работа с правами доступа к нескольким объектам

В этом разделе описано, как можно изменить права доступа сразу для нескольких объектов.

Меню Редактировать права доступа к объекту предназначено для работы с правами доступа к одному объекту. Команда Предоставить права доступа к объекту (GRTOBJAUT) позволяет изменить права доступа сразу для нескольких объектов. Команда GRTOBJAUT может выполняться в интерактивном или пакетном режиме. Ее можно вызывать в программах.

Ниже приведены примеры применения команды GRTOBJAUT и ее меню. Команда отправляет сообщения для каждого указанного объекта с информацией о том, было ли внесено изменение. Для изменения прав доступа к объекту требуется заблокировать этот объект в исключительном режиме, то есть изменение нельзя внести, когда объект используется. Для получения информации об удачном или неудачном изменении прав доступа напечатайте протокол задания.

- Для того чтобы предоставить всем объектам из библиотеки TESTLIB общие права доступа *USE, нужно ввести следующее:

```

                                Предоставить права доступа к объекту (GRTOBJAUT)
Введите опции, нажмите Enter.
Объект . . . . . *ALL
Библиотека . . . . . TESTLIB
Тип объекта . . . . . *ALL
ASP . . . . . *
Пользователи . . . . . *PUBLIC
+ доп. значения
Права доступа . . . . . *USE

```

Приведенная в примере команда GRTOBJAUT предоставляет указанные права доступа, но не аннулирует права доступа более высокого уровня. Если некоторым объектам из библиотеки TESTLIB были предоставлены общие права доступа *CHANGE, то эта команда не заменит их на права доступа *USE. Для того чтобы все объекты из библиотеки TESTLIB имели общие права доступа *USE, вызовите команду GRTOBJAUT с параметром REPLACE.

```

GRTOBJAUT OBJ(TESTLIB/*ALL) OBJTYPE(*ALL) +
USER(*PUBLIC) REPLACE(*YES)

```

Параметр REPLACE указывает, нужно ли заменить текущие права доступа пользователя на указанные права доступа. Значение по умолчанию REPLACE(*NO) предоставляет указанные права доступа, но не аннулирует существующие права доступа более высокого уровня. Исключение составляет только тот случай, когда предоставляются права доступа *EXCLUDE.

Указанные выше команды устанавливают общие права доступа только для тех объектов, которые уже существуют в библиотеке. Общие права доступа для объектов, которые будут создаваться в библиотеке в будущем, можно задать с помощью параметра CRTAUT из описания библиотеки.

- Предположим, что пользователям AMES и SMITHR нужно предоставить права доступа *ALL к рабочим файлам из библиотеки TESTLIB. В данном примере имена всех рабочих файлов начинаются с символов WRK:

```

                                Предоставить права доступа к объекту (GRTOBJAUT)
Введите опции, нажмите Enter.
Объект . . . . . WRK*
Библиотека . . . . . TESTLIB
Тип объекта . . . . . *FILE
ASP . . . . . *
Пользователи . . . . . AMES
+ для доп. значений SMITHR
Права доступа . . . . . *ALL

```

В этой команде файлы заданы с помощью шаблона. Шаблон представляет собой строку символов, которая заканчивается звездочкой (*). Информация о том, в каких параметрах команды разрешено указывать шаблон имени, приведена в электронной справке.

- Для того чтобы общие права доступа к файлам с именами вида AR* брались из списка прав доступа ARLST1, введите следующие команды:

1. Свяжите с файлами список прав доступа с помощью команды GRTOBJAUT:

```
Предоставить права доступа к объекту
Введите опции, нажмите Enter.
Объект . . . . . AR*
Библиотека . . . . . TESTLIB
Тип объекта . . . . . *FILE
ASP . . . . . *
:
Список прав доступа . . . . . ARLST1
```

2. Задайте для файлов общие права доступа *AUTL с помощью команды GRTOBJAUT:

```
Предоставить права доступа к объекту
Введите опции, нажмите Enter.
Объект . . . . . AR*
Библиотека . . . . . TESTLIB
Тип объекта . . . . . *FILE
ASP . . . . . *
Пользователи . . . . . *PUBLIC
+ доп. значения
Права доступа . . . . . *AUTL
```

Работа с принадлежностью объекта

В этом разделе описаны способы изменения принадлежности объекта.

Для изменения принадлежности объекта можно воспользоваться одной из следующих команд:

- Изменить владельца объекта (CHGOBJOWN)
- Работа с объектами по владельцу (WRKOBJOWN)
- Изменить владельца (CHGOWN)

В меню Работа с объектами по владельцу показаны все объекты, принадлежащие определенному профайлу. Отдельные объекты можно передать новому владельцу. Для того чтобы изменить принадлежность нескольких объектов, задайте параметр NEWOWN (Новый владелец), расположенный в нижней области меню:

Работа владельца с объектами

Пользовательский профайл : OLDDOWNER

Введите опции и нажмите Enter.

2=Изменить права доступа 4=Удалить 5=Показать автора
8=Показать описание 9=Изменить владельца

Опц	Объект	Библиотека	Тип	Атрибут	ASP
	COPGMSG	COPGLIB	*MSGQ		ASP *SYSBAS
9	CUSTMAS	CUSTLIB	*FILE		*SYSBAS
9	CUSTMSGQ	CUSTLIB	*MSGQ		*SYSBAS
	ITEMMSGQ	ITELIB	*MSGQ		*SYSBAS

Параметры или команда

====> **NEWOWN (OWNIC)**

F3=Выход F4=Приглашение F5=Обновить F9=Восстановить

F18=Конец

После изменения принадлежности объекта одним из указанных способов можно удалить права старого владельца объекта. Это делается по умолчанию, то есть по умолчанию параметру CUROWNAUT (Права доступа текущего владельца) присвоено значение *REVOKE.

Для изменения владельца объекта необходимы следующие права доступа:

- Права к существованию объекта
- Права доступа *ALL или права владельца, если объект является списком прав доступа
- Права на добавление по отношению к пользовательскому профайлу нового владельца
- Права на удаление по отношению к пользовательскому профайлу старого владельца

Если пользовательскому профайлу принадлежат какие-либо объекты, то его нельзя удалять. В разделе “Удаление пользовательских профайлов” на стр. 127 указано, что следует делать с объектами, принадлежащими удаляемому профайлу.

В меню Работа с объектами по владельцу среди прочих объектов показаны объекты интегрированной файловой системы. Для этих объектов в поле *Объект* указываются первые 18 символов полного имени. Если полное имя содержит более 18 символов, то в конце усеченного имени будет показан символ (>). Для просмотра полного пути поместите курсор в поле имени и нажмите клавишу F22.

Работа с правами доступа основной группы

В этом разделе описана процедура изменения основной группы или ее прав доступа к объекту.

Для изменения основной группы или ее прав доступа к объекту предназначены следующие команды:

- Изменить основную группу объекта (CHGOBJPGP)
- Работа с объектами по основной группе (WRKOBJPGP)
- Изменить основную группу (CHGPGP)

При изменении основной группы объекта указываются права доступа новой основной группы. При необходимости можно аннулировать права доступа старой основной группы. Если эти права доступа не будут аннулированы, они станут частными правами доступа.

Новая основная группа не должна являться владельцем объекта.

Для изменения основной группы объекта необходимы следующие права доступа:

- Права доступа *OBJEXIST по отношению к объекту
- Права доступа *OBJOPR и *OBJEXIST, если объект - это файл, библиотека или описание подсистемы.

- Специальные права доступа *ALLOBJ или права владельца объекта, если объект - это список прав доступа.
- Права доступа *OBJMGT, если требуется аннулировать права доступа старой основной группы.
- Права доступа *OBJMGT и все предоставляемые права доступа, если указанное значение отлично от *PRIVATE.

Работа с модельным объектом

Меню Редактировать права доступа к объекту и команда GRTOBJAUT позволяют предоставлять права доступа к объекту или группе объектов согласно модельному объекту.

Эту возможность очень удобно применять в ряде случаев, однако в качестве альтернативы следует рассмотреть возможность применения списка прав доступа. Преимущества применения списков прав доступа описаны в разделе “Преимущества списка прав доступа” на стр. 174.

Копирование прав доступа пользователя

Команда Предоставить права доступа пользователю (GRTUSRAUT) позволяет скопировать все частные права доступа из одного пользовательского профайла в другой.

Такой способ удобно использовать в ряде случаев. Например, в системе нельзя переименовать пользовательский профайл. Для создания аналогичного профайла с другим именем требуется выполнить ряд действий, в том числе скопировать права доступа исходного профайла. В “Переименование пользовательского профайла” на стр. 131 приведен пример выполнения этой операции.

Команда GRTUSRAUT копирует только частные права доступа. Она не копирует специальные права доступа и не изменяет владельца объекта.

Команду GRTUSRAUT не следует применять вместо создания профайлов групп. GRTUSRAUT создает копию набора частных прав доступа, что приводит к увеличению времени сохранения системы и усложняет управление правами доступа. Команда GRTUSRAUT копирует те права доступа, которые существуют в момент ее вызова. Если в будущем потребуются права доступа к другим объектам, то каждому профайлу эти права доступа нужно будет предоставлять по-отдельности. В профайле группы это делается автоматически.

Для применения команды GRTUSRAUT вам должны быть предоставлены все копируемые права доступа. Если у вас нет каких-либо прав доступа, то эти права доступа не будут предоставлены целевому профайлу. Система создает сообщения о том, какие права были или не были предоставлены. Для просмотра этих сообщений напечатайте протокол задания. Для того чтобы гарантированно были скопированы все права доступа, команда GRTUSRAUT должна быть запущена пользователем со специальными правами доступа *ALLOBJ.

Задачи, связанные с данной

“Копирование частных прав доступа” на стр. 127

Скопировать частные права доступа из одного пользовательского профайла в другой можно с помощью команды Предоставить пользователю права доступа (GRTUSRAUT).

Работа с списками прав доступа

В этом разделе описаны действия по созданию списка прав доступа.

Настройка списка прав доступа включает в себя три этапа:

1. Создание списка прав доступа.
2. Добавление пользователей в список прав доступа.
3. Настройка списка прав доступа для защиты объектов.

Шаги 2 и 3 могут выполняться в любом порядке.

Преимущества списка прав доступа

Для защиты объектов в системе могут использоваться списки прав доступа.

Списки прав доступа обладают следующими преимуществами:

- Упрощают управление правами доступа. Права доступа пользователя указываются в списке прав доступа, а не для каждого объекта в отдельности. Если список прав доступа настраивается для нового объекта, пользователи в списке автоматически получают права доступа к этому объекту.
- Позволяют предоставить права доступа ко всем объектам в списке с помощью одной операции.
- Сокращают количество частных прав доступа в системе. Каждому пользователю можно предоставить частные права доступа только к одному объекту - списку прав доступа. При этом пользователь получит правами доступа ко всем объектам в списке. Сокращение количества частных прав доступа в системе позволяет добиться:
 - Сокращения размера пользовательских профайлов.
 - Повышения производительность при выполнении команд сохранения системы (SAVSYS) и сохранения данных защиты (SAVSECDTA).
- Предоставляют эффективный способ защиты файлов. В случае частных прав доступа пользователю предоставляются частные права доступа к каждому элементу файла. При использовании списка прав доступа для каждого пользователя создается только одна запись прав доступа. Кроме того, частные права доступа не позволяют предоставить или аннулировать права доступа к открытому файлу. В случае списка прав доступа права можно изменять, даже если файл открыт.
- Позволяют сохранять информацию о правах доступа при сохранении объекта. Если с объектом связан список прав доступа, то имя этого списка сохраняется вместе с объектом. При восстановлении удаленного объекта в той же системе автоматически восстанавливается его связь со списком прав доступа. Если объект восстанавливается в другой системе, то связь со списком прав доступа восстанавливается только в том случае, если в команде восстановления задан параметр ALWOBJDIF(*ALL) или ALWOBJDIF(*AUTL).
- Список прав доступа - это самый удобный инструмент для управления доступом к объектам с одинаковыми требованиями к защите. Даже если список применяется для защиты небольшого числа объектов, работать с ним удобнее, чем с частными правами доступа к отдельным объектам. Поскольку все права доступа указываются в одном объекте (списке), он позволяет упростить предоставление и аннулирование прав доступа к объектам. Кроме того, он упрощает процедуру настройки прав доступа для новых объектов, когда эти права доступа совпадают с правами к существующим объектам.

Создание списка прав доступа

Команда Создать список прав доступа (CRTAUTL) позволяет создать список прав доступа.

Для создания списка прав доступа в библиотеке QSYS не требуются никакие права доступа к этой библиотеке. Достаточно вызвать команду Создать список прав доступа (CRTAUTL):

```
                Создать список прав доступа (CRTAUTL)
Введите опции, нажмите Enter.
Список прав доступа . . . . . cust1st1      Имя
Описание . . . . .
Файлы, очищаемые в конце месяца
                Дополнительные параметры
Права доступа . . . . . *use              *CHANGE, *ALL, *USE, *EXCLUDE
```

Параметр AUT задает общие права доступа для объектов, связанных со списком прав доступа. Общие права доступа из списка прав доступа применяются только в том случае, если общие права доступа к объекту равны *AUTL.

Предоставлению пользователям доступа к списку прав доступа

Меню Редактировать список прав доступа (EDTAUTL) позволяет изменить права доступа пользователя к списку прав доступа.

Для работы с правами доступа, предоставленными пользователям по отношению к списку прав доступа, необходимы права доступа *AUTLMGT (права на управление списком прав доступа) и все права доступа, которые вы планируете предоставить. Полная информация по этому вопросу приведена в разделе “Управление списком прав доступа” на стр. 145.

Меню Редактировать список прав доступа (EDTAUTL) позволяет изменить права доступа пользователя к списку прав доступа и добавить пользователей в список:

```

                                Редактировать список прав доступа
Объект . . . . . : CUSTLST1      Владелец . . . . . : PGMR1
Библиотека . . . . : QSYS        Основная группа . . . : *NONE

Измените текущие права доступа и нажмите Enter.

Пользоват     Права к     Упр
*PUBLIC       объекту   списком
              *USEPGMR1   *ALL      X

```

Для того чтобы предоставить пользователям права доступа к списку прав доступа, нажмите F6 (Добавить пользователей):

```

                                Добавить пользователей
Объект . . . . . : CUSTLST1      Владелец . . . PGMR1
Библиотека . . . . : QSYS

Укажите новых пользователей, нажмите Enter.

Пользоват     Права к     Упр
AMES          объекту   списком
SMITHR       *CHANGE

```

Права доступа пользователя к списку хранятся в пользовательском профайле как частные права доступа. Для работы с пользователями списка прав доступа в интерактивном или пакетном режиме можно использовать следующие команды:

- Добавить запись списка прав доступа (ADDAUTLE) - позволяет определить права доступа для нового пользователя.
- Изменить запись списка прав доступа (CHGAUTLE) - позволяет изменить текущие права доступа пользователя к списку.
- Удалить запись списка прав доступа (RMVAUTLE) - позволяет аннулировать права доступа пользователя к списку.
- Работа с правами доступа (WRKAUT) - позволяет просмотреть список пользователей, у которых есть права доступа к данному объекту.
- Изменить права доступа (CHGAUT) - позволяет изменить права доступа пользователя к данному объекту.

Настройка списка прав доступа для защиты объектов

Настраивать список прав доступа для защиты объекта может только владелец объекта, пользователь с правами доступа *ALL по отношению к этому объекту и пользователь со специальными правами доступа *ALLOBJ.

Список прав доступа можно настроить для защиты объекта с помощью меню Редактировать права доступа объекта или команды GRTOBJAUT, WRKAUT или CHGAUT:

```

                                Редактировать права доступа к объекту
Объект . . . . . : ARWRK1   Владелец . . . . . : PGMR1
Библиотека . . . : TESTLIB  Основная группа . . . : *NONE
Тип объекта . . . : *FILE    ASP. . . . . : *SYSBAS
Измените текущие права доступа и нажмите Enter.

    Объект защищен списком прав доступа . . . . . ARLST1

                Права доступа
Пользоват     к объекту
*PUBLIC              *AUTL
PGMR1              *ALL
```

Для того чтобы общие права доступа к объекту определялись списком прав доступа, укажите в поле общих прав доступа значение *AUTL.

В меню Редактировать список прав доступа можно просмотреть список всех объектов, для защиты которых применяется список. Для этого нужно нажать клавишу F15 (Показать объекты списка прав доступа).

```

                                Показать объекты списка прав доступа
Список прав доступа. . . . . : CUSTLST1
Библиотека . . . . . : CUSTLIB
Владелец . . . . . : OWNAR
Основная группа. . . . . : DPTAR

Объект      Библиотека  Тип      Владелец  Основная  Описание
CUSTMAS     CUSTLIB    *FILE    OWNAR     группа
CUSTADDR    CUSTLIB    *FILE    OWNAR
```

Этот список приводится только для вашего сведения. В нем нельзя добавлять и удалять объекты. Просмотреть и напечатать список всех объектов, для защиты которых применяется список прав доступа, можно и с помощью команды Показать объекты списка прав доступа (DSPAUTOBJ).

Настройка списка прав доступа

Список прав доступа позволяет управлять правами доступа к объектам и упрощает процедуру настройки прав доступа для новых объектов, когда эти права доступа совпадают с правами к существующим объектам.

В компании JKL Toys списки прав доступа служат для защиты всех рабочих файлов, которые применяются при учете в конце месяца. При этом выполняется очистка этих файлов, что требует наличия прав доступа *OBJMGT. Изменение требований к приложению может привести к появлению дополнительных рабочих файлов. Кроме того, при кадровых изменениях в компании могут меняться пользователи, запускающие операции ежемесячной обработки. Список прав доступа позволяет упростить внесение всех перечисленных изменений.

Ниже описана процедура настройки списка прав доступа.

1. Создайте список прав доступа:
CRTAUTL ICLIST1
2. Свяжите список со всеми рабочими файлами:
GRTOBJAUT OBJ(ITEMLIB/ICWRK*) +
OBJTYP(*FILE) AUTL(ICLIST1)

3. Добавьте в список пользователей, запускающих ежемесячные операции обработки:

```
ADDAUTLE AUTL(ICLIST1) USER(USERA) AUT(*ALL)
```

Если применяется список прав доступа, для объектов не следует указывать частные права доступа. В противном случае проверка частных прав доступа для объекта будет выполняться дважды. Вначале система проверит частные права доступа к объекту, а затем - частные права доступа к списку прав доступа. При этом будут использованы дополнительные системные ресурсы, что может повлиять на производительность системы. Если применяется только список прав доступа, то выполняется только одна операция поиска. Кроме того, поскольку при использовании списка прав доступа применяется кэширование прав, проверка будет выполняться с той же скоростью, что и обычная проверка частных прав доступа к объекту.

Удаление списка прав доступа

Созданный список прав доступа можно удалить.

Список прав доступа нельзя удалить до тех пор, пока он применяется для защиты каких-либо объектов. Для просмотра полного списка таких объектов введите команду DSPAUTLOBJ. Измените права доступа к указанным в списке объектам с помощью меню Редактировать права доступа к объекту, команды Изменить права доступа (CHGAUT) или команды Аннулировать права доступа к объекту (RVKOBJAUT). Когда не останется ни одного объекта, связанного со списком прав доступа, удалите список с помощью команды Удалить список прав доступа (DLTAUTL).

Как система проверяет права доступа

Когда пользователь пытается выполнить операцию над объектом, система проверяет его права доступа на выполнение этой операции.

Вначале система проверяет наличие прав доступа к библиотеке объекта или каталогам из пути к объекту. Если эти права доступа достаточны для выполнения операции, система проверяет права доступа к самому объекту. Для файлов баз данных проверка прав доступа выполняется во время открытия файла, а не при выполнении каждой операции над файлом.

Процедура проверки прав доступа прекращается, как только система обнаруживает какие-либо права доступа (даже если эти права доступа недостаточны для выполнения запрошенной операции). После этого система предоставляет или запрещает доступ исходя из найденных прав. Исключением являются принятые права доступа. Принятые права доступа переопределяют обычные права доступа, если их уровень недостаточен для выполнения операции. Дополнительная информация о принятых правах доступа приведена в разделе “Объекты, принимающие права доступа владельца” на стр. 156.

Система проверяет права доступа пользователя к объекту в следующей последовательности:

1. Права доступа к объекту - быстрая проверка
2. Специальные права доступа *ALLOBJ пользователя
3. Специальные права доступа пользователя к объекту
4. Права доступа пользователя в списке прав доступа, применяемом для защиты объекта
5. Специальные права доступа *ALLOBJ группы
6. Специальные права доступа группы к объекту
7. Права доступа группы в списке прав доступа, применяемом для защиты объекта
8. Общие права доступа, заданные для объекта или для списка прав доступа, применяемого для защиты объекта
9. Права доступа владельца программы, если используются принятые права доступа

Примечание: При поиске прав доступа пользователя к объекту могут быть объединены права доступа нескольких групп этого пользователя.

Блок-схемы проверки прав доступа

В этом разделе приведены блок-схемы, их описание и примеры проверки прав доступа.

С их помощью можно определить, будет ли работать та или иная схема прав доступа, а также обнаружить ошибку в применяемой схеме прав доступа. В блок-схемах особо выделены те типы прав доступа, которые сильнее всего влияют на производительность.

Весь процесс проверки прав доступа представлен в виде основной блок-схемы и нескольких мелких блок-схем, описывающих отдельные фрагменты процесса. В некоторых блок-схемах действия могут выполняться по несколько раз, в зависимости от сочетания прав доступа к объекту.

Номера, указанные в верхних левых углах блоков схемы, применяются в приведенных ниже примерах.

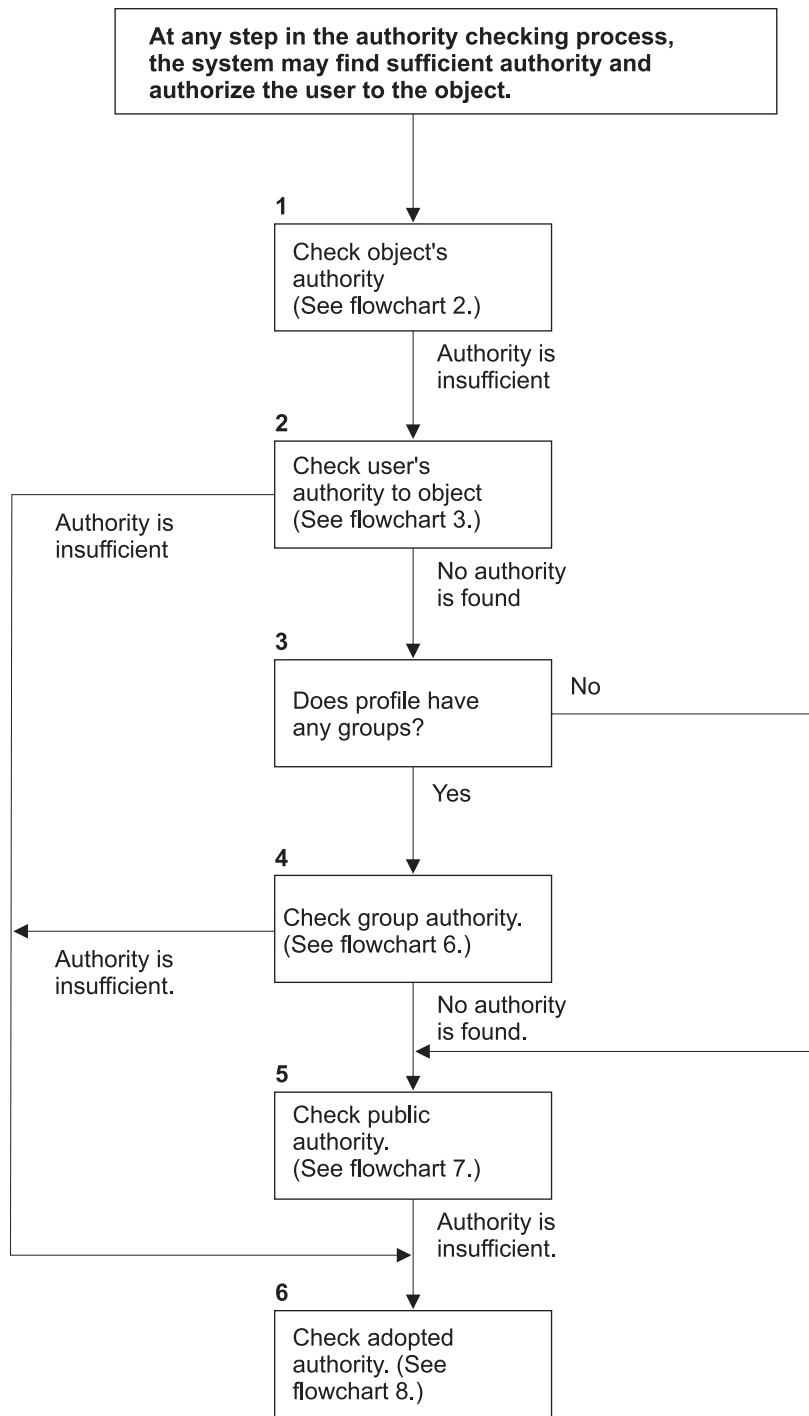
Ниже перечислены шаги, выполняемые для определения частных прав доступа профайла:

- Шаг 6 в рис. 13 на стр. 183
- Шаг 6 в рис. 16 на стр. 189
- Шаг 2 в рис. 19 на стр. 194

Повторение этих шагов с большой вероятностью приведет к снижению производительности процесса проверки прав доступа.

Блок-схема 1: Основной процесс проверки прав доступа

На блок-схеме 1 изображен основной процесс проверки прав доступа к объекту.



If the user is not authorized, one or more of the following happens:
 1) A message is sent to the user or program; 2) The program fails;
 3) An AF entry is written to the audit journal.

RBAFW508-1

Рисунок 11. Блок-схема 1: Основной процесс проверки прав доступа

Блок-схема 1: Основной процесс проверки прав доступа - Описание

Примечание: Система может обнаружить необходимые права доступа и предоставить доступ к объекту на любом шаге проверки прав доступа.

1. Система проверяет права доступа к объекту. (Обратитесь к Блок-схеме 2: Быстрая проверка прав доступа к объекту.) Если на этом шаге не будут найдены достаточные права доступа, то система перейдет к шагу 2.
2. Система проверяет права доступа к объекту, предоставленные пользователю. (Обратитесь к Блок-схеме 3: Проверка прав доступа пользователя к объекту.) Если пользователю не предоставлены права доступа к объекту, то система переходит к шагу 3. Если пользователю предоставлены недостаточные права доступа, то система переходит к шагу 6.
3. Система проверяет, входит ли пользовательский профайл в какую-либо группу. Если да, то система переходит к шагу 4. Если нет, то система переходит к шагу 5.
4. Система проверяет права доступа группы. (Обратитесь к блок-схеме 6). Если группе не предоставлены права доступа к объекту, то система переходит к шагу 5. Если группе предоставлены недостаточные права доступа к объекту, то система переходит к шагу 6.
5. Система проверяет общие права доступа к объекту. (Обратитесь к блок-схеме 7.) Если общих прав доступа недостаточно для выполнения операции, то система переходит к шагу 6.
6. Система проверяет принятые права доступа. (Обратитесь к блок-схеме 8.)

Блок-схема 2: Быстрая проверка прав доступа к объекту

На блок-схеме 2 изображен процесс проверки информации, хранящейся в объекте. Такая проверка позволяет быстрее всего предоставить пользователю доступ к объекту.



Рисунок 12. Блок-схема 2: Быстрая проверка прав доступа к объекту

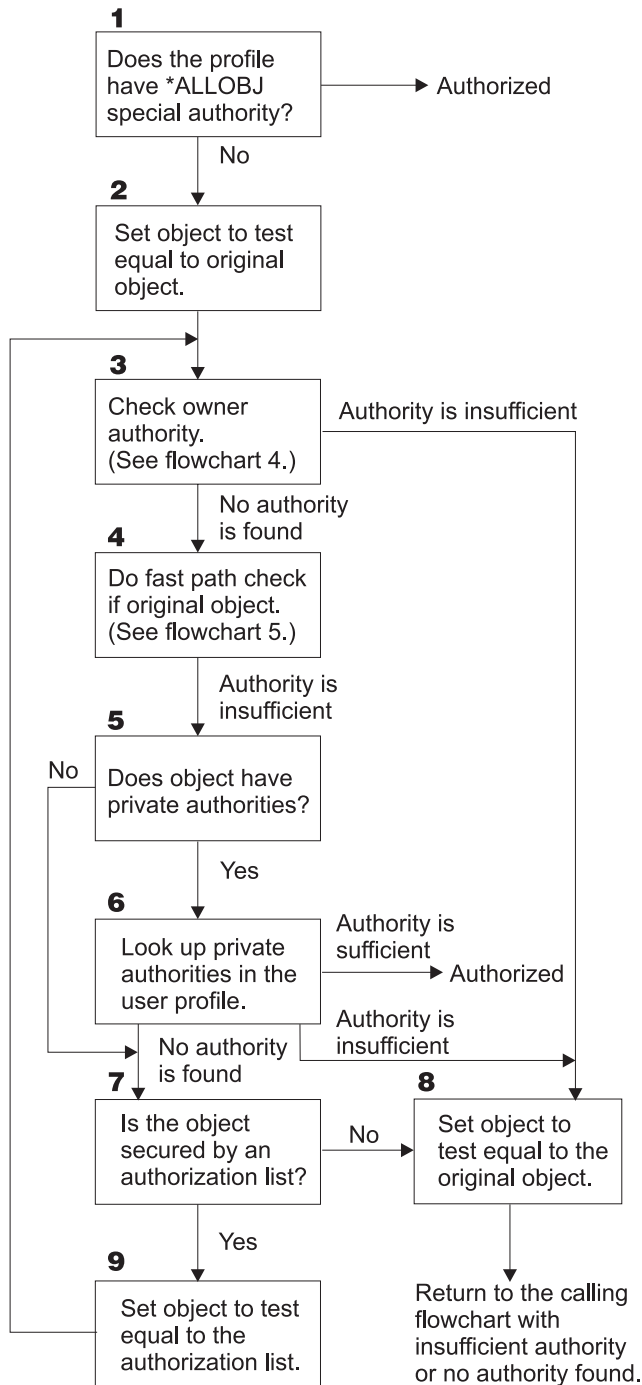
Блок-схема 2: Быстрая проверка прав доступа к объекту - Описание

1. Система проверяет, определены ли частные права доступа к объекту. Если да, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии достаточных прав доступа. Если нет, то система переходит к шагу 2.
2. Система проверяет, защищен ли объект с помощью списка прав доступа. Если да, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии достаточных прав доступа. Если нет, то система переходит к шагу 3.
3. Система проверяет, предоставлены ли необходимые права доступа владельцу объекта. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии достаточных прав доступа. Если да, система переходит к шагу 4.
4. Система проверяет, определена ли для объекта основная группа. Если да, то система переходит к шагу 5. Если нет, то система переходит к шагу 6.
5. Система проверяет, предоставлены ли необходимые права доступа основной группе объекта. Если да, то система переходит к шагу 6. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии необходимых прав доступа.

6. Система проверяет, достаточно ли общих прав доступа для выполнения операции. Если да, то доступ к объекту предоставляется. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии достаточных прав доступа.

Блок-схема 3: Проверка прав доступа пользователя к объекту

Все действия, описанные в блок-схеме 3, выполняются над профайлом отдельного пользователя.



RBAFW523-1

Рисунок 13. Блок-схема 3: Проверка прав доступа пользователя

Блок-схема 3: Проверка прав доступа пользователя - Описание

1. Система проверяет, предоставлены ли пользовательскому профайлу права доступа *ALLOBJ. Если да, то профайлу предоставляется доступ к объекту. Если нет, то система переходит к шагу 2.
2. Система устанавливает для тестового объекта права доступа, совпадающие с правами доступа к исходному объекту. Система переходит к шагу 3.

3. Система проверяет права доступа владельца. Если этих прав доступа недостаточно, то система переходит к шагу 8. Если такие права доступа не предоставлены, то система переходит к шагу 4.
4. Система выполняет быструю проверку прав доступа для исходного объекта. (Обратитесь к блок-схеме 5.) Если прав доступа недостаточно, то система переходит к шагу 5.
5. Система проверяет, заданы ли частные права доступа к объекту. Если да, то система переходит к шагу 6. Если нет, то система переходит к шагу 7.
6. Система проверяет частные права доступа для пользовательского профайла. Если профайлу предоставлены достаточные права доступа, то система разрешает доступ к объекту. Если профайлу предоставлены недостаточные права доступа, то система переходит к шагу 8. Если профайлу не предоставлены права доступа, то система переходит к шагу 7.
7. Система проверяет, защищен ли объект с помощью списка прав доступа. Если нет, то система переходит к шагу 8. Если да, то система переходит к шагу 9.
8. Система устанавливает в качестве тестируемого объекта исходный объект и возвращается к исходной блок-схеме с результатом, свидетельствующим о недостаточных правах доступа или об отсутствии прав доступа.
9. Система устанавливает в качестве тестируемого объекта список прав доступа и возвращается к шагу 3.

Блок-схема 4: Проверка прав доступа владельца

На блок-схеме 4 представлен процесс проверки прав доступа владельца. Имя профайла владельца и права доступа владельца хранятся вместе с объектом.

Существует несколько случаев, в которых права доступа владельца позволяют получить доступ к объекту:

- Пользовательскому профайлу принадлежит объект.
- Пользовательскому профайлу принадлежит список прав доступа.
- Профайлу группы пользователя принадлежит объект.
- Профайлу группы пользователя принадлежит список прав доступа.
- Программа использует принятые права доступа, и владельцу программы принадлежит объект.
- Программа использует принятые права доступа, и владельцу программы принадлежит список прав доступа.

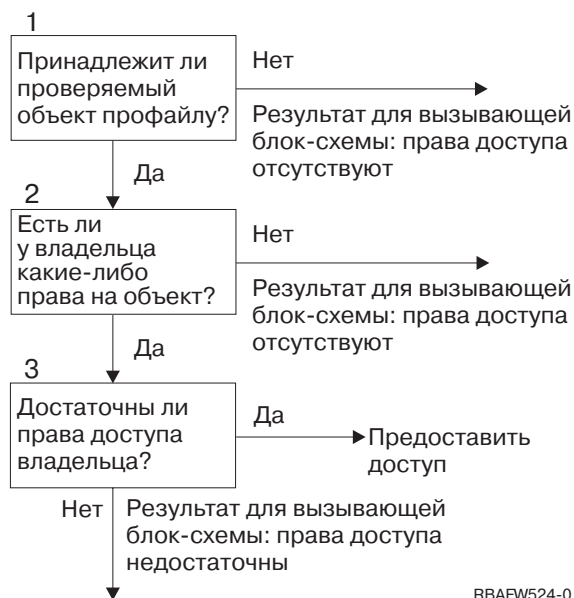


Рисунок 14. Блок-схема 4: Проверка прав доступа владельца

Блок-схема 4: Проверка прав доступа владельца - Описание

1. Система проверяет, принадлежит ли объект пользовательскому профайлу. Если да, то система переходит к шагу 2. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа.
2. Если объект принадлежит пользовательскому профайлу, то система проверяет наличие прав доступа к объекту. Если владельцу предоставлены права доступа, то система переходит к шагу 3. Если владельцу не предоставлены права доступа к объекту, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа.
3. Если владельцу предоставлены права доступа к объекту, то система проверяет, достаточно ли этих прав доступа. Если прав доступа достаточно, то система разрешает доступ к объекту. Если прав доступа недостаточно, то система возвращается к исходной блок-схеме с результатом, свидетельствующим о наличии недостаточных прав доступа.

Блок-схема 5: Быстрая проверка прав доступа пользователя

Блок-схема 5 иллюстрирует быстрый способ проверки прав доступа пользователя, не требующий определения частных прав доступа.

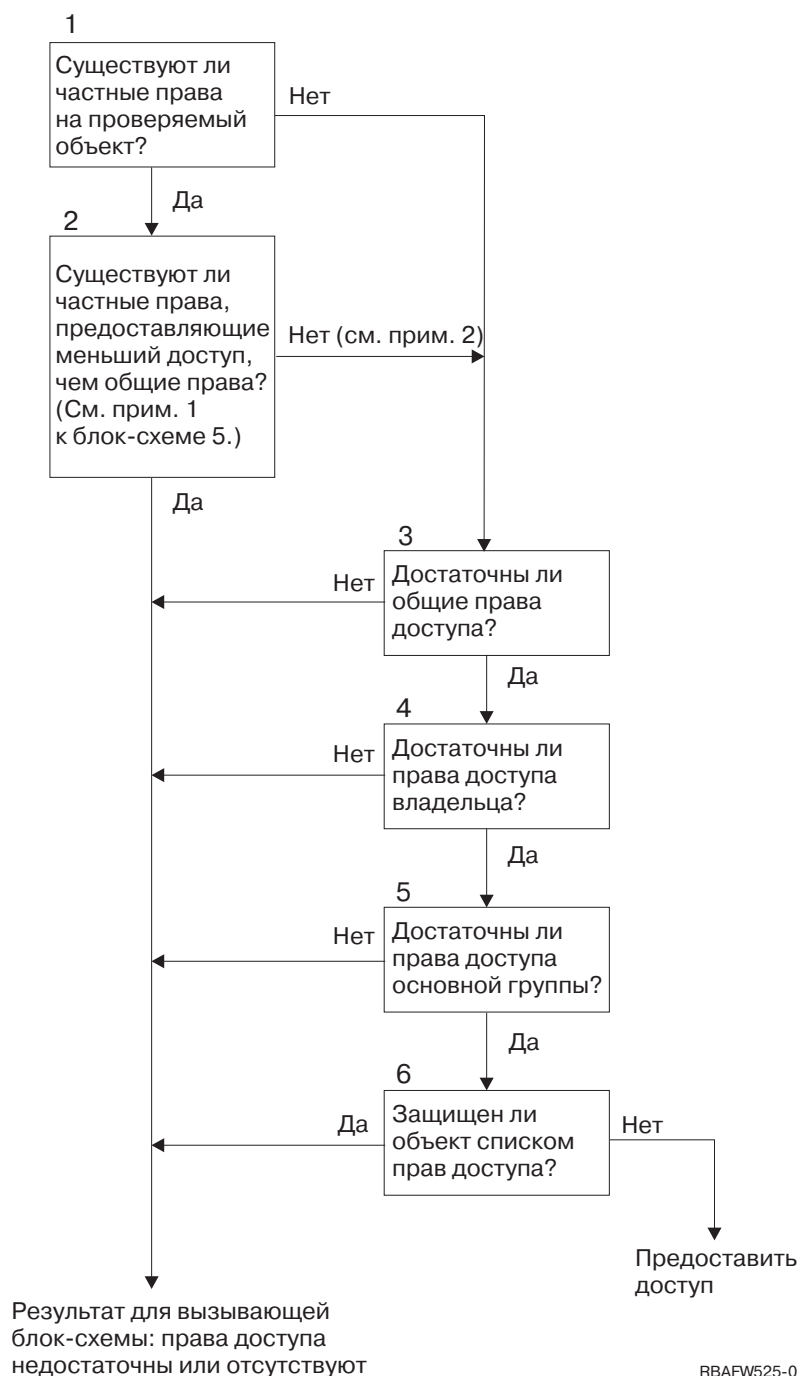


Рисунок 15. Блок-схема 5: Быстрая проверка прав доступа пользователя

Примечания к блок-схеме 5:

1. Считается, что права доступа ниже уровня общих прав доступа, если какие-либо из прав доступа *PUBLIC не предоставлены отдельному пользователю. В примере из раздела Табл. 121 на стр. 187 общие права доступа включают в себя права доступа *OBJOPR, *READ и *EXECUTE. Пользователю WILSONJ предоставлены права доступа *EXCLUDE и не предоставлены никакие из общих прав доступа. Следовательно, частные права доступа к объекту ниже уровня общих прав доступа. (Права доступа OWNER также ниже уровня общих прав доступа, однако права владельца не относятся к категории частных прав доступа.)

Таблица 121. Общие и частные права доступа

Права доступа	Пользователи			
	OWNER	DPTMG	WILSONJ	*PUBLIC
<i>Права доступа к объекту:</i>				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
<i>Права доступа к данным</i>				
*READ		X		X
*ADD		X		
*UPD		X		
*DLT		X		
*EXECUTE		X		X
*EXCLUDE			X	

2. Быстрый поиск позволяет использовать общие права доступа (если это возможно) даже при наличии частных прав доступа к объекту. Система выполняет ряд тестов, для того чтобы убедиться в том, что ничто в дальнейшем процессе проверки прав доступа не запрещает доступ к объекту. Если в результате этих тестов будет получено значение *Права доступа достаточно*, то поиск частных прав доступа можно пропустить.

Блок-схема 5: Быстрая проверка прав доступа пользователя - Описание

На блок-схеме показан быстрый способ проверки прав доступа пользователя, не требующий определения частных прав доступа.

1. Система проверяет, заданы ли частные права доступа к объекту. Если да, то система переходит к шагу 2. Если нет, то система переходит к шагу 3.
2. Если частные права доступа заданы, система сравнивает уровень этих прав доступа с уровнем общих прав доступа. (См. примечание 1.) Если уровень частных прав доступа к объекту ниже уровня общих прав доступа, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа или наличии недостаточных прав доступа. Если уровень частных прав доступа к объекту не ниже уровня общих прав доступа (см. примечание 2), то система переходит к шагу 3.
3. Система проверяет, достаточно ли общих прав доступа к объекту для выполнения операции, если частные права доступа отсутствуют или недостаточны. Если да, то система переходит к шагу 4. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа или наличии недостаточных прав доступа.
4. Система проверяет, достаточно ли прав доступа владельца объекта для выполнения операции. Если да, то система переходит к шагу 5. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа или наличии недостаточных прав доступа.
5. Система проверяет, достаточно ли прав доступа основной группы объекта для выполнения операции. Если да, то система переходит к шагу 6. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа или наличии недостаточных прав доступа.
6. Система проверяет, применяется ли список прав доступа для защиты объекта. Если да, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа или наличии недостаточных прав доступа. Если нет, то пользователю предоставляется доступ к объекту.

Блок-схема 6: Проверка прав доступа группы

Пользователь может входить в состав не более 16 групп. Группе могут быть предоставлены частные права доступа к объекту, либо она может быть назначена основной группой объекта.

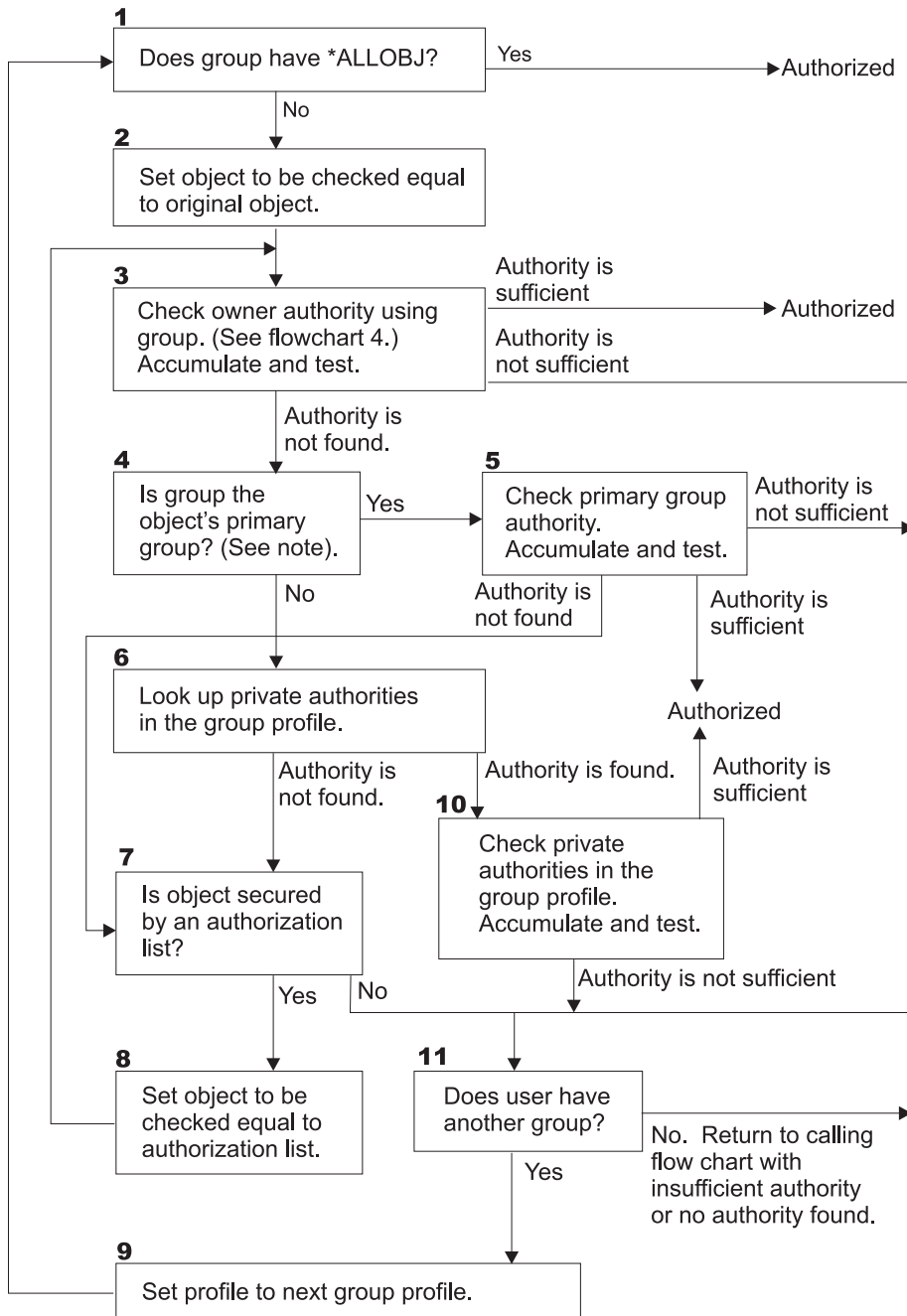
При поиске прав доступа пользователя к объекту могут быть объединены права доступа нескольких групп этого пользователя. Например, пользователю WAGNERB необходимы права доступа *CHANGE к файлу CRLIM. В группу прав доступа *CHANGE входят права доступа *OBJOPR, *READ, *ADD, *UPD, *DLT и *EXECUTE. В таблице Табл. 122 показаны права доступа к файлу CRLIM:

Таблица 122. Совокупные права доступа группы

Права доступа	Пользователи			
	OWNER	DPT506	DPT702	*PUBLIC
<i>Права доступа к объекту:</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
<i>Права доступа к данным</i>				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X	X	
*DLT	X		X	
*EXECUTE	X	X	X	
*EXCLUDE				X

Для получения необходимых прав доступа к файлу CRLIM пользователю WAGNERB необходимы как права доступа DPT506, так и права доступа DPT702. У DPT506 нет прав доступа *DLT, а у DPT702 нет прав доступа *ADD.

Блок-схема 6 на странице рис. 16 на стр. 189 демонстрирует процедуру проверки прав доступа групп.



RBAFW509-1

Рисунок 16. Блок-схема 6: Проверка прав доступа группы

Примечание: Если пользователь вошел в систему с использованием профайла, назначенного основной группой объекта, то он не может получить права доступа к объекту путем их наследования от основной группы.

Блок-схема 6: Проверка прав доступа группы - Описание

- | 1. Система проверяет, предоставлены ли группе права доступа *ALLOBJ. Если да, то группе предоставляется доступ к объекту. Если нет, то система переходит к шагу 2.
- | 2. Если у группы нет прав доступа *ALLOBJ, система задает исходный объект в качестве проверяемого объекта.

3. Система проверяет права доступа владельца (обратитесь к блок-схеме 4). Если этих прав доступа достаточно, то группе предоставляется доступ к объекту. Если прав доступа недостаточно, то система переходит к шагу 11. При отсутствии таких прав доступа система переходит к шагу 4.
4. Если права доступа владельца не были найдены, то система проверяет, является ли группа основной группой объекта.

Примечание: Если пользователь вошел в систему с использованием профайла, назначенного основной группой объекта, то он не может получить права доступа к объекту путем их наследования от основной группы.

Если группа является основной группой объекта, то система переходит к шагу 5. Если группа не является основной группой объекта, то система переходит к шагу 6.

5. Система проверяет права доступа основной группы. Если прав доступа основной группы достаточно для выполнения операции, то группе предоставляется доступ к объекту. Если отсутствуют права доступа основной группы, то система переходит к шагу 7. Если этих прав доступа недостаточно, то система переходит к шагу 11.
6. Если группа не является основной группой объекта, то система проверяет наличие частных прав доступа в профайле группы. При наличии таких прав доступа система переходит к шагу 10. При отсутствии таких прав доступа система переходит к шагу 7.
7. Если профайлу группы не предоставлены частные права доступа, то система проверяет, задан ли для объекта список прав доступа. Если да, то система переходит к шагу 8. Если нет, то система переходит к шагу 11.
8. Если для защиты объекта применяется список прав доступа, то система устанавливает список прав доступа в качестве проверяемого объекта и возвращается к шагу 3.
9. Если пользователь входит еще в одну группу, то система делает текущим профайл следующей группы и возвращается к шагу 1, чтобы начать процесс проверки заново.
10. Если профайлу группы предоставлены частные права доступа, то система выполняет их проверку. Если прав доступа достаточно для выполнения операции, то профайлу группы предоставляется доступ к объекту. Если прав доступа недостаточно, то система переходит к шагу 11.
11. Если права доступа отсутствуют или недостаточны, то система проверяет, входит ли пользователь в другие группы. Если пользователь входит в другой профайл группы, то система переходит к шагу 9. Если нет, то система возвращается к исходной блок-схеме с результатом, свидетельствующим об отсутствии прав доступа или наличии недостаточных прав доступа.

Блок-схема 7: Проверка общих прав доступа

Перед проверкой общих прав доступа система должна определить, какие права доступа следует использовать: общие права доступа к объекту или список прав доступа.

Выполнение этой процедуры описывает блок-схема 7:



Рисунок 17. Блок-схема 7: Проверка общих прав доступа

Блок-схема 7: Проверка общих прав доступа - Описание

На блок-схеме 7 показано, как система определяет, какие права доступа нужно использовать: общие права доступа к объекту или список прав доступа.

1. Система проверяет, задано ли в качестве общих прав доступа к исходному объекту значение *AUTL. Если да, то система переходит к шагу 2. Если нет, то система переходит к шагу 3.
2. Система заменяет проверяемый объект на список прав доступа и переходит к шагу 4.
3. Система заменяет проверяемый объект на исходный объект и переходит к шагу 4.
4. Если в качестве проверяемого объекта был задан список прав доступа или исходный объект, то система проверяет, достаточно ли общих прав доступа. Если общих прав доступа достаточно, то пользователю предоставляется доступ к объекту. Если общих прав доступа недостаточно, то система возвращается к исходной блок-схеме с результатом, свидетельствующим о наличии недостаточных прав доступа.

Блок-схема 8: Проверка принятых прав доступа

Если проверка прав доступа пользователя показала, что пользователю предоставлены недостаточные права доступа, то система проверяет принятые права доступа.

Это могут быть права доступа, принятые той программой, которую вызвал пользователь, или права доступа, принятые предыдущими программами из стека вызовов. Для повышения производительности и сокращения количества операций поиска частных прав доступа система проверяет, предоставлены ли владельцу программы специальные права доступа *ALLOBJ или права владельца проверяемого объекта. Эта операция выполняется для каждой программы из стека, использующей принятые права доступа.

Если необходимые права доступа не были найдены, система проверяет, предоставлены ли владельцу программы частные права доступа к проверяемому объекту. Эта операция выполняется для каждой программы из стека, использующей принятые права доступа.

На рис. 18 на стр. 192 и рис. 19 на стр. 194 показан процесс проверки принятых прав доступа.

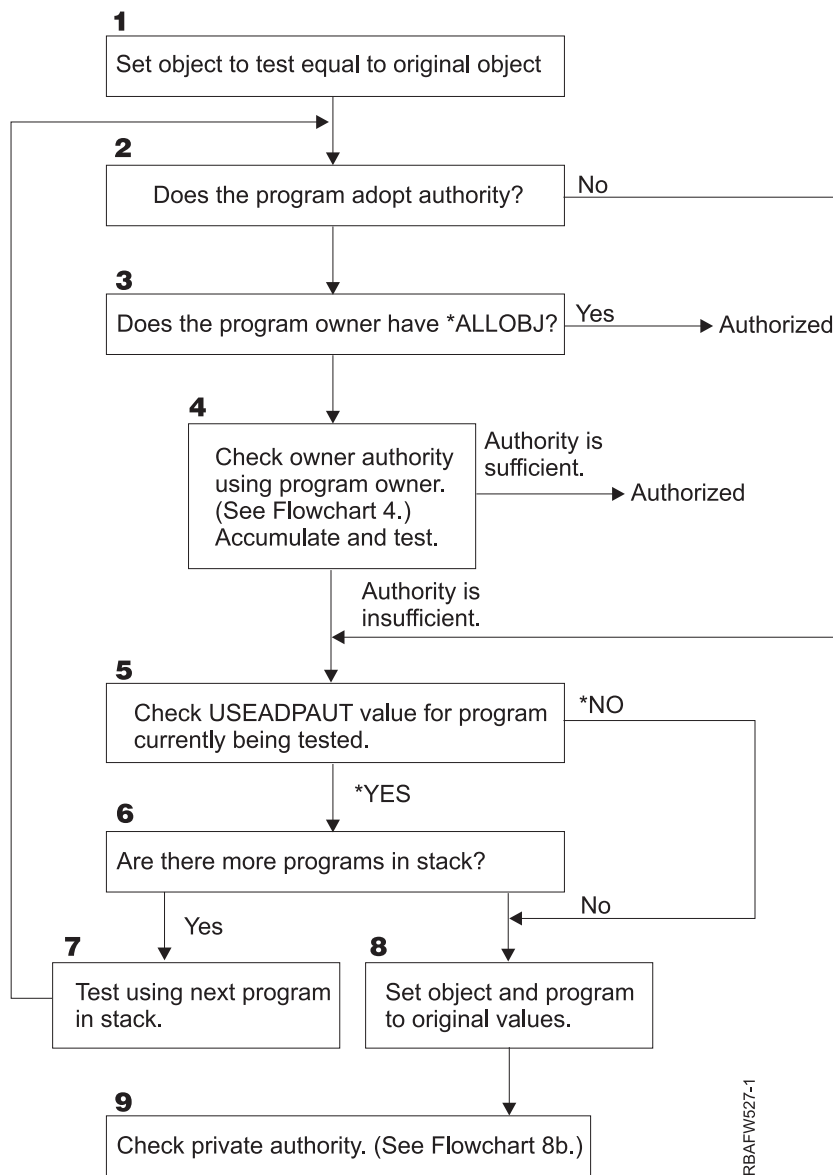


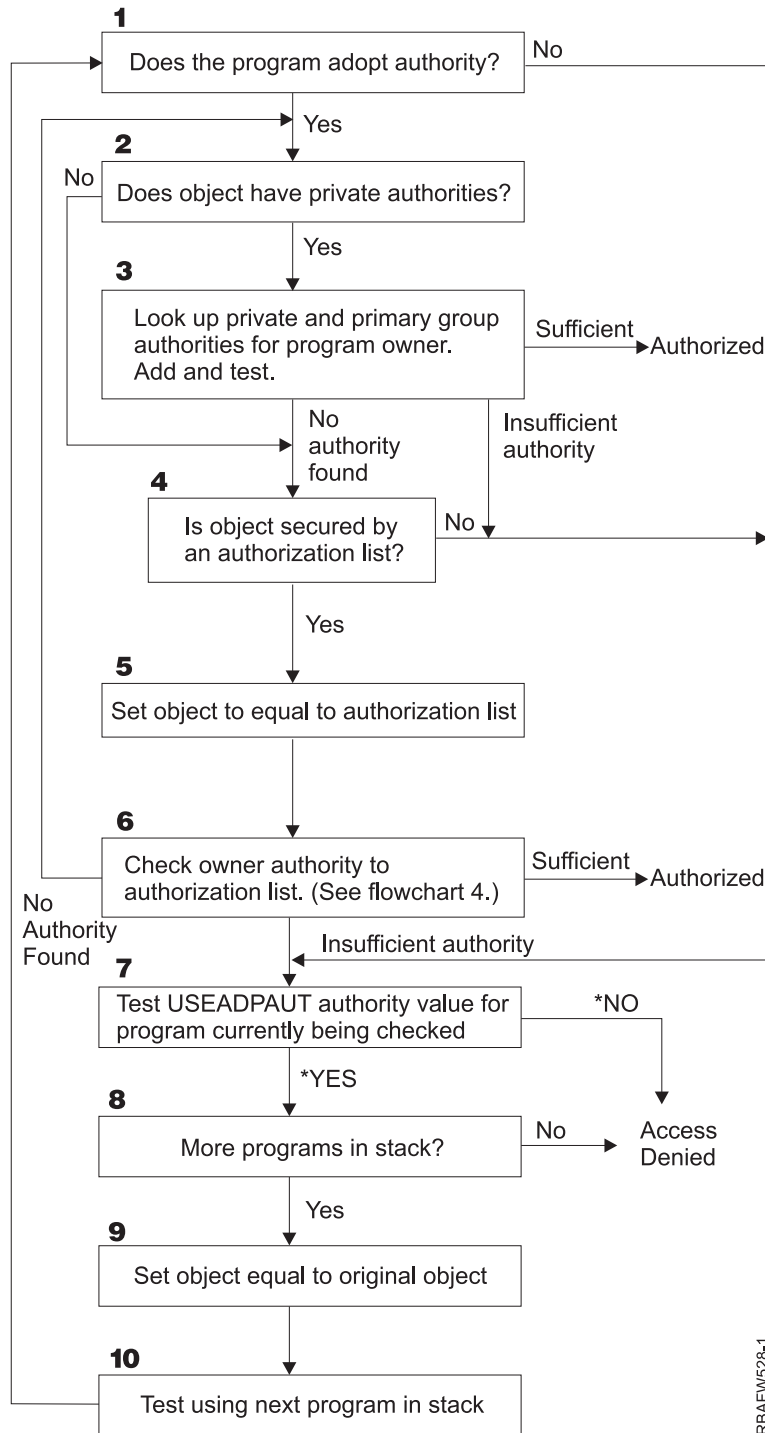
Рисунок 18. Блок-схема 8А: Проверка принятых прав доступа пользователя *ALLOBJ или владельца

Блок-схема 8А: Проверка принятых прав доступа пользователя *ALLOBJ или владельца - Описание

Блок-схема 8А описывает процесс проверки принятых прав доступа, выполняемый в том случае, если прав доступа пользователя недостаточно для выполнения операции.

1. Система устанавливает в качестве проверяемого объекта исходный объект и переходит к шагу 2.
2. Система проверяет, принимает ли программа права доступа. Если да, то система переходит к шагу 3. Если нет, то система переходит к шагу 5.
3. Если программа принимает права доступа, система проверяет, предоставлены ли владельцу программы права доступа *ALLOBJ. Если да, то пользователю предоставляется доступ к объекту. Если нет, то система переходит к шагу 4.
4. Если владельцу программы не предоставлены права доступа *ALLOBJ, то система проверяет его права доступа. Если профайлу предоставлены достаточные права доступа, то система разрешает доступ к объекту. Если предоставлены недостаточные права доступа, то система переходит к шагу 5.

5. Система проверяет значение параметра USEADPAUT текущей программы. Если оно равно *NO, то система переходит к шагу 8. Если оно равно *YES, то система переходит к шагу 6.
6. Если значение параметра USEADPAUT равно *YES, то система проверяет наличие других программ в стеке. Если в стеке есть другие программы, то система переходит к шагу 7. Если в стеке нет других программ, ожидающих проверки, то система переходит к шагу 8.
7. Система выбирает следующую программу в стеке и возвращается к шагу 2.
8. Если в стеке не осталось ни одной непроверенной программы, и значение параметра USEADPAUT равно *NO, то система устанавливает в качестве объекта и программы исходные значения и переходит к шагу 9.
9. Система проверяет частные права доступа. Эта процедура показана на рисунке Блок-схема 8В: Проверка принятых прав доступа с помощью частных прав доступа.



RBAFW528-1

Рисунок 19. Блок-схема 8В: Проверка принятых прав доступа с помощью частных прав доступа

Блок-схема 8В: Проверка принятых прав доступа с помощью частных прав доступа - Описание

1. Система проверяет, может ли программа принимать права доступа. Если да, система переходит к шагу 2. Если нет, система переходит к шагу 7.
2. Система проверяет, предоставлены ли объекту частные права доступа. Если да, система переходит к шагу 3. Если нет, система переходит к шагу 4.

3. Система проверяет частные права доступа владельца программы и права доступа основной группы. Если этих прав доступа достаточно, то программе предоставляется доступ. Если этих прав доступа недостаточно, то система переходит к шагу 7. Если права доступа не были найдены, то система переходит к шагу 4.
4. Система проверяет, защищен ли объект с помощью списка прав доступа. Если да, система переходит к шагу 5. Если нет, система переходит к шагу 7.
5. Система устанавливает в качестве проверяемого объекта список прав доступа и переходит к шагу 6.
6. Система проверяет права доступа, предоставленные владельцу по отношению к списку прав доступа. (Обратитесь к блок-схеме 4.) Если права доступа не предоставлены, система возвращается к шагу 2. Если права доступа достаточны для выполнения операции, то программе предоставляется доступ.
7. Система проверяет значение параметра USEADPAUT текущей программы. Если оно равно *YES, система переходит к шагу 8. Если оно равно *NO, то система запрещает доступ.
8. Система проверяет наличие непроверенных программ в стеке. Если такие программы есть, система переходит к шагу 9. Если таких программ нет, то система запрещает доступ.
9. Система устанавливает в качестве проверяемого объекта исходный объект и переходит к шагу 10.
10. Система выбирает следующую программу в стеке и возвращается к шагу 1.

Понятия, связанные с данным

“Игнорирование принятых прав доступа” на стр. 245

При применении принятых прав доступа в проектировании меню пользователю необходимо перейти в начальное меню. Для того чтобы пользователи могли запускать запросы как с помощью начального меню, так и с помощью меню приложений, настройте программу QRYSTART для игнорирования принятых прав доступа.

Примеры проверки прав доступа

В этом разделе приведено несколько примеров проверки прав доступа.

Эти примеры демонстрируют, каким образом система проверяет, разрешен ли пользователю запрошенный тип доступа к объекту. С их помощью можно понять, каким образом выполняется процедура проверки прав доступа и что может послужить причиной снижения производительности.

На рис. 20 указаны права доступа к файлу PRICES. После рисунка приведено несколько примеров обращений к файлу и процедур проверки прав доступа. В этих примерах особо отмечен поиск частных прав доступа (блок-схема 4, шаг 6), так как многократное выполнение этого фрагмента процесса проверки прав доступа может привести к снижению производительности.

Показать права доступа к объекту

```

Объект . . . . . : PRICES      Владелец . . . . . : OWNCP
Библиотека . . . . : CONTRACTS  Основная группа. . . : *NONE
Тип объекта . . . . : *FILE      ASP. . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. . . : *NONE

Профайл      Группа      Права доступа
к объекту
OWNCP
DPTSM        *CHANGE
DPTMG        *CHANGE
WILSONJ      *USE
*PUBLIC      *USE

```

Рисунок 20. Права доступа к файлу PRICES

Пример 1: Применение частных прав доступа группы

В это примере описано применение частных прав доступа.

Пользователь ROSSM попытался обратиться к файлу PRICES с помощью программы CPPGM01. Программе CPPGM01 необходимы права доступа *CHANGE к файлу. ROSSM входит в состав группы DPTSM. Ни пользователю ROSSM, ни группе DPTSM не предоставлены специальные права доступа *ALLOBJ. Для того чтобы выяснить, следует ли разрешить пользователю ROSSM доступ к файлу PRICES, система выполняет следующие действия:

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаг 1.
2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = CONTRACTS/PRICES *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Возврат к блок-схеме 3, так как права доступа не найдены. Файл PRICES не принадлежит пользователю ROSSM.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаги 1, 2 и 3. Общих прав доступа недостаточно.
 - d. Блок-схема 3, шаг 5.
 - e. Блок-схема 3, шаг 6. Пользователю ROSSM не предоставлены частные права доступа к файлу PRICES.
 - f. Блок-схема 3, шаги 7 и 8. Для защиты файла PRICES не применяется список прав доступа. Возврат к блок-схеме 1, так как права доступа не найдены.
3. Блок-схема 1, шаги 3 и 4. DPTSM является группой пользователя ROSSM.
 - a. Блок-схема 6, шаги 1, 2 и 3.
 - 1) Блок-схема 4, шаг 1. Файл PRICES не принадлежит группе DPTSM.
 - b. Блок-схема 6, шаг 4. DPTSM не является основной группой файла PRICES.
 - c. Блок-схема 6, шаг 6. Доступ разрешен. (Группе DPTSM предоставлены права доступа *CHANGE.)

Результат:

Пользователю ROSSM разрешен доступ, так как профайлу группы DPTSM предоставлены права доступа *CHANGE.

Анализ:

В данном примере права доступа группы являются хорошим способом управления доступом. Данный способ сокращает количество частных прав доступа в системе. Он прост для понимания и его легко контролировать. Однако применение частных прав доступа группы обычно требует дважды выполнять поиск частных прав доступа (для пользователя и для группы), если общих прав доступа недостаточно. Одну операцию поиска частных прав доступа можно исключить, назначив группу DPTSM основной группой файла PRICES.

Пример 2: Применение прав доступа основной группы

В это примере описано применение прав доступа основной группы.

Пользователю ANDERSJ требуются права доступа *CHANGE к файлу CREDIT. ANDERSJ входит в состав группы DPTAR. Ни пользователю ANDERSJ, ни группе DPTAR не предоставлены специальные права доступа *ALLOBJ. На рис. 21 на стр. 197 показаны права доступа к файлу CREDIT.

Показать права доступа к объекту			
Объект :	CREDIT	Владелец :	OWNER
Библиотека :	ACCTSRVC	Основная группа. :	DPTAR
Тип объекта :	*FILE	ASP. :	*SYSBAS
Объект защищен списком прав доступа :			
. . . :	*NONE		
Профайл	Группа	Права доступа к объекту	
OWNER		*ALL	
DPTAR		*CHANGE	
*PUBLIC		*USE	

Рисунок 21. Права доступа к файлу CREDIT

Для того чтобы узнать, следует ли предоставить пользователю ANDERSJ доступ к файлу CREDIT для выполнения операции *CHANGE, система выполняет следующие действия:

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаг 1. Группе DPTAR предоставлены права доступа основной группы, а не частные права доступа.
 - b. Блок-схема 2, шаги 2, 3, 4, 5 и 6. Общих прав доступа недостаточно.
2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = ACCTSRVC/CREDIT *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл CREDIT не принадлежит пользователю ANDERSJ. Возврат к блок-схеме 3, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаг 1. Для файла CREDIT не заданы частные права доступа.
 - 2) Блок-схема 5, шаг 3. Общих прав доступа недостаточно. Возврат к блок-схеме 3, так как права доступа не найдены.
 - d. Блок-схема 3, шаги 5, 7 и 8. Для защиты файла CREDIT не применяется список прав доступа. Возврат к блок-схеме 1, так как права доступа не найдены.
3. Блок-схема 2, шаги 3 и 4. ANDERSJ входит в состав группы DPTAR.
 - a. Блок-схема 6, шаги 1 и 2. Проверяемый объект = ACCTSRVC/CREDIT *FILE.
 - b. Блок-схема 6, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл CREDIT не принадлежит группе DPTAR. Возврат к блок-схеме 6, так как права доступа не найдены.
 - c. Блок-схема 6, шаги 4 и 5. Доступ разрешен. DPTAR является основной группой файла CREDIT, и ей предоставлены права доступа *CHANGE.

Результат:

Пользователю ANDERSJ разрешен доступ, так как группа DPTAR является основной группой файла CREDIT, и ей предоставлены права доступа *CHANGE.

Анализ:

В случае прав доступа основной группы проверка прав доступа выполняется быстрее, чем в случае частных прав доступа группы. В данном примере не потребовалось выполнить ни одну операцию поиска частных прав доступа.

Понятия, связанные с данным

“Замечания об основной группе объектов” на стр. 252

Для любого объекта системы можно задать основную группу. Если основная группа объекта является первой группой большинства пользователей этого объекта, то, задав права доступа для основной группы, можно повысить производительность системы.

Пример 3: Применение общих прав доступа

В этом примере описаны действия по применению общих прав доступа.

Пользователь JONESP попытался обратиться к файлу CREDIT с помощью программы CPPGM06. Программе CPPGM06 необходимы права доступа *USE к файлу. Пользователь JONESP входит в состав группы DPTSM. Ему не предоставлены специальные права доступа *ALLOBJ. Для того чтобы выяснить, следует ли разрешить пользователю JONESP доступ к файлу CREDIT, система выполняет следующие действия:

Блок-схема 1, шаг 1.

1. Блок-схема 2, шаг 1. Для файла CREDIT не заданы частные права доступа. Группе DPTAR предоставлены права доступа основной группы, а не частные права доступа.
2. Блок-схема 2, шаги 2 и 3. Прав доступа владельца (OWNER) достаточно для выполнения операции.
3. Блок-схема 2, шаги 4 и 5. Прав доступа основной группы (DPTAR) достаточно для выполнения операции.
4. Блок-схема 2, шаг 6. Доступ разрешен. Общих прав доступа достаточно для выполнения операции.

Анализ:

Этот пример демонстрирует выигрыш в производительности, которого можно достичь, отказавшись от присвоения частных прав доступа к объекту.

Пример 4: Применение общих прав доступа без поиска частных прав доступа

В этом примере описано применение общих прав доступа без поиска частных прав доступа.

Пользователь JONESP попытался обратиться к файлу PRICES с помощью программы CPPGM06. Программе CPPGM06 необходимы права доступа *USE к файлу. Пользователь JONESP входит в состав группы DPTSM. Ему не предоставлены специальные права доступа *ALLOBJ. Для того чтобы выяснить, следует ли разрешить пользователю JONESP доступ к файлу PRICES, система выполняет следующие действия:

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаг 1. Для файла PRICES заданы частные права доступа.
2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = CONTRACTS/PRICES *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл PRICES не принадлежит пользователю JONESP. Возврат к блок-схеме 3, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаги 1, 2 и 3. Общих прав доступа достаточно для выполнения операции.
 - 2) Блок-схема 5, шаг 4. Прав доступа владельца достаточно для выполнения операции. (OWNCP предоставлены права доступа *ALL.)
 - 3) Блок-схема 5, шаг 5. Для файла PRICES не задана основная группа.
 - 4) Блок-схема 5, шаг 6. Доступ разрешен. (Для защиты файла PRICES не применяется список прав доступа.)

Анализ:

Этот пример демонстрирует выигрыш в производительности, которого можно достичь, отказавшись от присвоения частных прав доступа, уровень которых ниже уровня общих прав доступа, к объекту. Хотя для файла PRICES и установлены частные права доступа, для выполнения запроса достаточно общих прав доступа, поэтому поиск частных прав доступа не требуется.

Пример 5: Применение принятых прав доступа

В этом примере показаны преимущества работы с принятыми правами доступа, связанные с производительностью.

Пользователь SMITHG попытался обратиться к файлу PRICES с помощью программы CPPGM08. SMITHG не входит ни в одну группу пользователей. Ему не предоставлены специальные права доступа *ALLOBJ. Программе CPPGM08 необходимы права доступа *CHANGE к файлу. CPPGM08 принадлежит профайлу OWNCP и принимает права доступа своего владельца (параметр USRPRF равен *OWNER).

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаг 1.
2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = CONTRACTS/PRICES *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл PRICES не принадлежит пользователю SMITHG. Возврат к блок-схеме 3, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаги 1, 2 и 3. Общих прав доступа недостаточно.
 - d. Блок-схема 3, шаг 5.
 - e. **Блок-схема 3, шаг 6.** Пользователю SMITHG не предоставлены частные права доступа.
 - f. Блок-схема 3, шаги 7 и 8. Для защиты файла PRICES не применяется список прав доступа. Возврат к блок-схеме 1, так как права доступа не найдены.
3. Блок-схема 1, шаг 3. Пользователь SMITHG не входит ни в одну группу.
4. Блок-схема 1, шаг 5.
 - a. Блок-схема 7, шаг 1. Общие права доступа не равны *AUTL.
 - b. Блок-схема 7, шаг 3. Проверяемый объект = CONTRACTS/PRICES *FILE.
 - c. Блок-схема 7, шаг 4. Общих прав доступа недостаточно.
5. Блок-схема 1, шаг 6.
 - a. Блок-схема 8A, шаг 1. Проверяемый объект = CONTRACTS/PRICES *FILE.
 - b. Блок-схема 8A, шаги 2 и 3. Пользователю OWNCP не предоставлены права доступа *ALLOBJ.
 - c. Блок-схема 8A, шаг 4.
 - 1) Блок-схема 4, шаги 1, 2 и 3. Доступ разрешен. Пользователь OWNCP является владельцем файла PRICES, и ему предоставлены необходимые права доступа.

Анализ:

Этот пример демонстрирует выигрыш в производительности, которого можно достичь за счет использования принятых прав доступа в тех случаях, когда владельцу программы принадлежат объекты приложения.

Число шагов, требуемых для проверки прав доступа, не оказывает существенного влияния на производительность, так как на большинстве из них не нужно получать новую информацию. Несмотря на большое число шагов, в данном примере поиск частных прав доступа выполняется только один раз (для пользователя SMITHG).

Сравните этот пример с примером 1, приведенным на странице “Пример 1: Применение частных прав доступа группы” на стр. 195.

- Если бы в примере 1 профайл группы DPTSM являлся владельцем файла PRICES и имел права доступа *ALL по отношению к этому файлу, то его уровень производительности был бы сравним с уровнем производительности данного примера. Однако назначение профайла группы владельцем объектов приложения представляет потенциальную угрозу для защиты. Элементам группы всегда будут предоставлены те же права доступа, что и самой группе (т.е. права владельца), если вы явно не предоставите им права доступа более низкого уровня. В случае применения принятых прав доступа вы можете решать, в каких случаях должны использоваться права владельца.
- Пример 1 можно изменить и таким образом, чтобы группа DPTSM являлась основной группой файла PRICES и имела права доступа *CHANGE по отношению к этому файлу. Если DPTSM - это первая группа файла SMITHG, указанная в параметре GRPPRF пользовательского профайла SMITHG, то уровень производительности примера 1 будет совпадать с уровнем производительности примера 5.

Пример 6: Права доступа пользователя и группы

Этот пример демонстрирует ситуацию, в которой пользователю не предоставляется доступ к объекту, несмотря на то, что у его группы есть достаточные права доступа к объекту.

Пользователь WILSONJ попытался обратиться к файлу PRICES с помощью программы CPPGM01, которой необходимы права доступа *CHANGE. WILSONJ входит в состав группы DPTSM. Ему не предоставлены специальные права доступа *ALLOBJ. Программа CPPGM01 не использует принятые права доступа и игнорирует ранее принятые права доступа (параметр USEADPAUT равен *NO).

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаг 1. Для файла PRICES заданы частные права доступа.
2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = CONTRACTS/PRICES *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл PRICES не принадлежит пользователю WILSONJ. Возврат к блок-схеме 3, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаги 1, 2 и 3. Общих прав доступа недостаточно.
 - d. Блок-схема 3, шаг 5.
 - e. **Блок-схема 3, шаг 6.** Пользователю WILSONJ предоставлены права доступа *USE, однако их недостаточно для выполнения операции.
 - f. Блок-схема 3, шаг 8. Проверяемый объект = CONTRACTS/PRICES *FILE. Возврат к блок-схеме 1, так как прав доступа недостаточно.
3. Блок-схема 1, шаг 6.
 - a. Блок-схема 8A, шаг 1. Проверяемый объект = CONTRACTS/PRICES *FILE.
 - b. Блок-схема 8A, шаг 2. Программа CPPGM01 не принимает права доступа.
 - c. Блок-схема 8A, шаг 5. Параметр *USEADPAUT программы CPPGM01 равен *NO.
 - d. Блок-схема 8A, шаги 8 и 9.
 - 1) Блок-схема 8B, шаг 1. Программа CPPGM01 не принимает права доступа.
 - 2) Блок-схема 8B, шаг 7. Параметр *USEADPAUT программы CPPGM01 равен *NO. Доступ запрещен.

Анализ:

Назначение пользователю прав доступа, уровень которых совпадает с уровнем общих прав доступа, но меньше уровня прав доступа группы, не влияет на производительность проверки прав доступа других пользователей. Однако если бы пользователю WILSONJ были присвоены права доступа *EXCLUDE (уровень которых ниже, чем уровень общих прав доступа), то продемонстрированный в примере 4 выигрыш в производительности был бы утерян.

Хотя этот пример состоит из большого числа шагов, поиск общих прав доступа выполняется только один раз. Это означает, что производительность будет приемлемой.

Пример 7: Общие права доступа без частных прав доступа

В этом примере продемонстрированы преимущества применения общих прав доступа при отсутствии частных прав доступа.

Для файла ITEM установлены следующие права доступа:

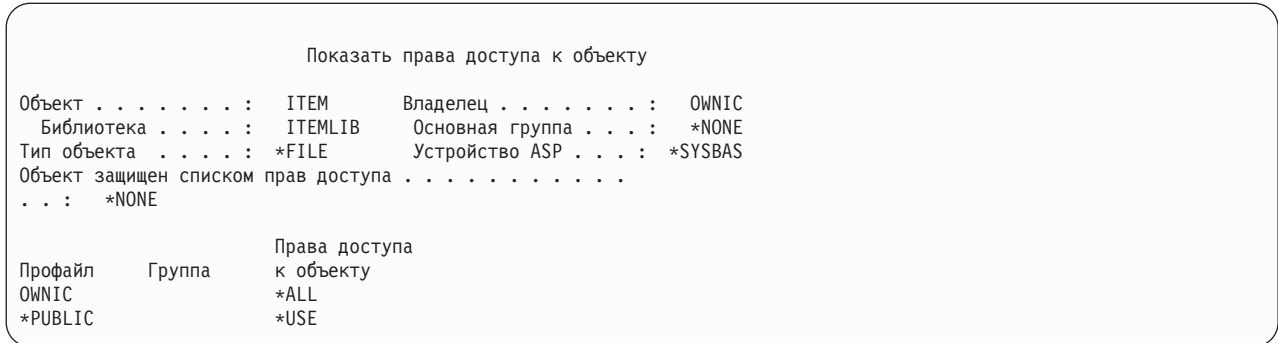


Рисунок 22. Показать права доступа к объекту

Пользователю ROSSM необходимы права доступа *USE к файлу ITEM. ROSSM входит в состав группы DPTSM. При проверке прав доступа выполняются следующие шаги:

Блок-схема 1, шаг 1.

1. Блок-схема 2, шаги 1, 2 и 3. Прав доступа пользователя OWNIC достаточно для выполнения операции.
2. Блок-схема 2, шаг 4. Для файла ITEM не задана основная группа.
3. Блок-схема 2, шаг 6. Доступ разрешен. Общих прав доступа достаточно для выполнения операции.

Анализ:

Общие права доступа обеспечивают максимальную производительность в тех случаях, когда не заданы никакие частные права доступа. В данном примере поиск частных прав доступа не выполняется ни разу.

Пример 8: Принятые права доступа без частных прав доступа

В этом примере продемонстрированы преимущества применения принятых прав доступа при отсутствии частных прав доступа.

В данном примере все программы приложения принадлежат профайлу OWNIC. Любая программа, которой необходимы права доступа более высокого уровня, чем *USE, принимает права доступа владельца. Пользователь WILSONJ попытался обратиться к файлу ITEM с помощью программы ICPGM10, принимающей права доступа. Ему необходимы права доступа *CHANGE. Процедура проверки прав доступа выглядит следующим образом:

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаги 1, 2, 3, 4 и 6. Общих прав доступа недостаточно.
2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = ITEM LIB/ITEM *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл ITEM не принадлежит пользователю WILSONJ. Возврат к блок-схеме 3, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.

- 1) Блок-схема 5, шаги 1 и 3. Общих прав доступа недостаточно. Возврат к блок-схеме 3, так как права доступа не найдены.
- d. Блок-схема 3, шаги 5, 7 и 8. Для защиты файла ITEM не применяется список прав доступа. Возврат к блок-схеме 1, так как права доступа не найдены.
- 3. Блок-схема 1, шаги 3 и 5. (Пользователь WILSONJ не входит ни в одну группу.)
 - a. Блок-схема 7, шаги 1, 3 и 4. Общие права доступа равны *USE. Их недостаточно для выполнения операции.
- 4. Блок-схема 1, шаг 6.
 - a. Блок-схема 8A, шаг 1. Проверяемый объект = ITEM LIB/ITEM *FILE.
 - b. Блок-схема 8A, шаги 2, 3 и 4. Профайлу OWNIC не предоставлены права доступа *ALLOBJ.
 - 1) Блок-схема 4, шаги 1, 2 и 3. Доступ разрешен. Профайлу OWNIC предоставлены необходимые права доступа к файлу ITEM.

Анализ:

В этом примере продемонстрированы преимущества применения принятых прав доступа при отсутствии частных прав доступа, в частности в тех случаях, когда владельцу программ принадлежат объекты приложения. В этом примере не требуется выполнять поиск частных прав доступа.

Пример 9: Применение списка прав доступа

В этом примере проиллюстрированы преимущества работы со списками прав доступа.

Для защиты файла ARWRK01 из библиотеки CUSTLIB применяется список прав доступа ARLST1. В рис. 23 и рис. 24 показаны права доступа:

```

                          Показать права доступа к объекту
Объект . . . . . : ARWRK01      Владелец . . . . . : OWNAR
Библиотека . . . . : CUSTLIB     Основная группа . . . . : *NONE
Тип объекта . . . . : *FILE      ASP. . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. . . : ARLST1

Профайл   Группа      Права доступа
OWNCP     *ALL
*PUBLIC   *USE
  
```

Рисунок 23. Права доступа к файлу ARWRK01

```

                          Показать список прав доступа
Объект . . . . . : ARLST1      Владелец . . . . . : OWNAR
Библиотека . . . . : QSYS       Основная группа . . . . : *NONE

Пользоват  Группа      Права к   Упр
OWNCP     *ALL
AMESJ     *CHANGE
*PUBLIC   *USE
  
```

Рисунок 24. Права доступа из списка прав доступа ARLST1

Пользователю AMESJ, не входящему ни в одну группу, необходимы права доступа *CHANGE к файлу ARWRK01. При проверке прав доступа выполняются следующие шаги:

- 1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаги 1 и 2. Для защиты файла ARWRK01 применяется список прав доступа.

2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = CUSTLIB/ARWRK01 *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл ARWRK01 не принадлежит пользователю AMESJ. Возврат к блок-схеме 2, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаги 1 и 3. Общих прав доступа недостаточно. Возврат к блок-схеме 3, так как права доступа не найдены.
 - d. Блок-схема 3, шаги 5, 7 и 9. Проверяемый объект = ARLST1 *AUTL.
 - e. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Список прав доступа ARLST1 не принадлежит пользователю AMESJ. Возврат к блок-схеме 3, так как права доступа не найдены.
 - f. Блок-схема 3, шаги 4 и 5.
 - g. Блок-схема 3, шаг 6. Доступ разрешен. Пользователю AMESJ предоставлены права доступа *CHANGE к списку прав доступа ARLST1.

Анализ:

Этот пример показывает, что список прав доступа значительно упрощает управление правами доступа и обеспечивает высокую производительность. В частности, это верно в тех случаях, когда для объектов, защищенных с помощью списка прав доступа, не настроены частные права доступа.

Если бы пользователь AMESJ входил в состав группы, то в примере увеличилось бы число шагов, но не число операций поиска частных прав доступа, так как для файла ARWRK01 не определены частные права доступа. Снижение производительности возможно в том случае, когда частные права доступа и списки прав доступа применяются в сочетании с правами доступа группы, как описано в разделе “Пример 11: Сочетание различных типов прав доступа” на стр. 204.

Пример 10: Применение нескольких групп

В этом примере описано применение нескольких групп.

Пользователю WOODBC необходимы права доступа *CHANGE к файлу CRLIM. WOODBC входит в состав трех групп: DPTAR, DPTSM и DPTMG. DPTAR - это первый профайл группы (GRPPRF). DPTSM и DPTMG - это дополнительные профайлы групп (SUPGRPPRF). На рис. 25 показаны права доступа к файлу CRLIM:

Показать права доступа к объекту

```

Объект . . . . . : CRLIM          Владелец . . . . . : OWNER
Библиотека . . . . : CUSTLIB      Основная группа . . . : DPTAR
Тип объекта . . . . : *FILE        ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. . . : *NONE

Профайл   Группа   Права доступа
OWNER     DPTAR     *ALL
DPTAR     DPTSM     *CHANGE
DPTSM     DPTMG     *USE
*PUBLIC   *PUBLIC   *EXCLUDE
    
```

Рисунок 25. Права доступа к файлу CRLIM

При проверке прав доступа выполняются следующие шаги:

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаг 1. Возврат к исходной блок-схеме, так как прав доступа недостаточно.

2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = CUSTLIB/CRLIM *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл CRLIM не принадлежит пользователю WOODBC. Возврат к блок-схеме 3, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаги 1, 2 и 3. Общих прав доступа недостаточно.
 - d. Блок-схема 3, шаг 5.
 - e. Блок-схема 3, шаг 6. Пользователю WOODBC не предоставлены никакие права доступа к файлу CRLIM.
 - f. Блок-схема 3, шаги 7 и 8. Для защиты файла CRLIM не применяется список прав доступа. Возврат к блок-схеме 1, так как права доступа не найдены.
3. Блок-схема 1, шаги 3 и 4. Первая группа WOODBC - DPTAR.
 - a. Блок-схема 6, шаги 1 и 2. Проверяемый объект = CUSTLIB/CRLIM *FILE.
 - b. Блок-схема 6, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл CRLIM не принадлежит DPTAR. Возврат к блок-схеме 6, так как права доступа не найдены.
 - c. Блок-схема 6, шаги 4 и 5. Доступ разрешен. Группа DPTAR является основной группой, и ей предоставлены необходимые права доступа.

Пример 11: Сочетание различных типов прав доступа

В этом примере описана неверная схема работы с правами доступа.

Пользователю WAGNERB необходимы права доступа *ALL к файлу CRLIMWRK. WAGNERB входит в состав трех групп: DPTSM, DPT702 и DPTAR. DPTSM - первая группа пользователя WAGNERB (GRPPRF). Права доступа к файлу CRLIMWRK показаны на рис. 26.

```

Показать права доступа к объекту
Объект . . . . . : CRLIMWRK      Владелец . . . . . : OWNER
Библиотека . . . . : CUSTLIB      Основная группа . . . : *NONE
Тип объекта . . . . : *FILE        ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. . . : CRLST1

Профайл      Группа      Права доступа
OWNER        *ALL
DPTSM        *USE
WILSONJ      *EXCLUDE
*PUBLIC      *USE

```

Рисунок 26. Права доступа к файлу CRLIMWRK

Для защиты файла CRLIMWRK применяется список прав доступа CRLST1. На рис. 27 на стр. 205 показаны права доступа из списка CRLST1.

Показать список прав доступа			
Объект :	CRLST1	Владелец :	OWNAR
Library :	QSYS	Основная группа :	DPTAR
Пользоват	Группа	Права к к объекту	Упр списком
OWNAR		*ALL	X
DPTAR		*ALL	
*PUBLIC		*EXCLUDE	

Рисунок 27. Права доступа из списка прав доступа CRLST1

Этот пример демонстрирует многие возможности проверки прав доступа. Кроме того, он показывает, что наличие большого количества вариантов прав доступа к объекту может отрицательно сказаться на производительности.

Для проверки прав доступа пользователя WAGNERB к файлу CRLIMWRK выполняются следующие шаги:

1. Блок-схема 1, шаг 1.
 - a. Блок-схема 2, шаг 1.
2. Блок-схема 1, шаг 2.
 - a. Блок-схема 3, шаги 1 и 2. Проверяемый объект = CUSTLIB/CRLIMWRK *FILE.
 - b. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл CRLIMWRK не принадлежит пользователю WAGNERB. Возврат к блок-схеме 3, так как права доступа не найдены.
 - c. Блок-схема 3, шаг 4.
 - 1) Блок-схема 5, шаги 1 и 2. Пользователю WILSONJ предоставлены права доступа *EXCLUDE, уровень которых ниже уровня общих прав доступа (*USE).
 - d. Блок-схема 3, шаги 5 и 6 (**первый поиск частных прав доступа**). Пользователю WAGNERB не предоставлены частные права доступа.
 - e. Блок-схема 3, шаги 7 и 9. Проверяемый объект = CRLST1 *AUTL.
 - f. Блок-схема 3, шаг 3.
 - 1) Блок-схема 4, шаг 1. Объект CRLST1 не принадлежит WILSONJ. Возврат к блок-схеме 3, так как права доступа не найдены.
 - g. Блок-схема 3, шаги 4 и 5.
 - h. Блок-схема 3, шаг 6 (**второй поиск частных прав доступа**). Пользователю WAGNERB не предоставлены частные права доступа к CRLST1.
 - i. Блок-схема 3, шаги 7 и 8. Проверяемый объект = CUSTLIB/CRLIMWRK *FILE.
3. Блок-схема 1, шаги 3 и 4. Первый профайл группы WAGNERB - DPTSM.
 - a. Блок-схема 6, шаги 1 и 2. Проверяемый объект = CUSTLIB/CRLIMWRK *FILE.
 - b. Блок-схема 6, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл CRLIMWRK не принадлежит DPTSM. Возврат к блок-схеме 6, так как права доступа не найдены.
 - c. Блок-схема 6, шаг 4. DPTSM не является основной группой файла CRLIMWRK.
 - d. Блок-схема 6, шаг 6 (**третий поиск частных прав доступа**). Группе DPTSM предоставлены права доступа *USE к файлу CRLIMWRK, которых недостаточно для выполнения операции.
 - e. Блок-схема 6, шаг 6 (продолжение). К найденным правам доступа групп WAGNERB (таких прав доступа нет) добавляются права доступа *USE. Прав доступа недостаточно.
 - f. Блок-схема 6, шаги 9 и 10. Следующая группа WAGNERB - DPT702.
 - g. Блок-схема 6, шаги 1 и 2. Проверяемый объект = CUSTLIB/CRLIMWRK *FILE.
 - h. Блок-схема 6, шаг 3.

- 1) Блок-схема 4, шаг 1. Файл CRLIMWRK не принадлежит DPT702. Возврат к блок-схеме 6, так как права доступа не найдены.
- i. Блок-схема 6, шаг 4. DPT702 не является основной группой файла CRLIMWRK.
- j. Блок-схема 6, шаг 6 (**четвертый поиск частных прав доступа**). Группе DPT702 не предоставлены права доступа к файлу CRLIMWRK.
- k. Блок-схема 6, шаги 7 и 8. Проверяемый объект = CRLST1 *AUTL
- l. Блок-схема 6, шаг 3.
 - 1) Блок-схема 5, шаг 1. Список прав доступа CRLST1 не принадлежит DPT702. Возврат к блок-схеме 6, так как права доступа не найдены.
- m. Блок-схема 6, шаги 4 и 6. (**пятый поиск частных прав доступа**). DPT702 не предоставлены права доступа к списку CRLST1.
- n. Блок-схема 6, шаги 7, 9 и 10. Следующая группа WAGNERB - DPTAR.
- o. Блок-схема 6, шаги 1 и 2. Проверяемый объект = CUSTLIB/CRLIMWRK *FILE.
- p. Блок-схема 6, шаг 3.
 - 1) Блок-схема 4, шаг 1. Файл CRLIMWRK не принадлежит группе DPTAR. Возврат к блок-схеме 6, так как права доступа не найдены.
- q. Блок-схема 6, шаги 4 и 6. (**шестой поиск частных прав доступа**). Группе DPTAR не предоставлены права доступа к файлу CRLIMWRK.
- r. Блок-схема 6, шаги 7 и 8. Проверяемый объект = CRLST1 *AUTL
- s. Блок-схема 6, шаг 3.
 - 1) Блок-схема 4, шаг 1. Список прав доступа CRLST1 не принадлежит DPTAR. Возврат к блок-схеме 6, так как права доступа не найдены.
- t. Блок-схема 6, шаги 4 и 5. Доступ разрешен. Группа DPTAR является основной группой списка прав доступа CRLST1, и ей предоставлены права доступа *ALL.

Результат:

Пользователю WAGNERB разрешено выполнить запрошенную операцию, используя права доступа, предоставленные основной группе (DPTAR) по отношению к списку прав доступа CRLST1.

Анализ:

В этом примере продемонстрирована схема прав доступа, которая плоха как с точки зрения управления правами доступа, так и с точки зрения производительности. В схеме использовано слишком много различных вариантов прав доступа, что делает ее запутанной и неудобной для изменения и контроля. Поиск частных прав доступа выполняется шесть раз, что может привести к существенному снижению производительности:

Профайл	Объект	Тип	Результат
WAGNERB	CRLIMWRK	*FILE	Права доступа не найдены
WAGNERB	CRLST1	*AUTL	Права доступа не найдены
DPTSM	CRLIMWRK	*FILE	*USE (прав доступа недостаточно)
DPT702	CRLIMWRK	*FILE	Права доступа не найдены
DPT702	CRLST1	*AUTL	Права доступа не найдены
DPTAR	CRLIMWRK	*FILE	Права доступа не найдены

Для повышения производительности в этом примере достаточно изменить последовательность профайлов групп пользователя WAGNERB. Предположим, что DPTAR - это первый профайл группы пользователя

WAGNERB (GRPPRF). В этом случае система трижды проверит частные права доступа, прежде чем обнаружит, что DPTAR предоставлены права доступа основной группы по отношению к списку прав доступа CRLST1:

- Права доступа WAGNERB к файлу CRLIMWRK
- Права доступа WAGNERB к списку прав доступа CRLST1
- Права доступа DPTAR к файлу CRLIMWRK

Из этого примера можно сделать вывод о том, что для обеспечения высокой производительности системы необходимо тщательно планировать создание групп и списков прав доступа.

Кэш прав доступа

Система создает кэши прав доступа для пользователей, позволяющие работать более гибко и с большей производительностью.

Начиная с версии 3, выпуска 7 система создает кэш прав доступа при первом обращении пользователя к объекту. При последующих обращениях к объекту система выполняет поиск прав доступа в пользовательском кэше, и лишь затем - в пользовательском профайле. Это позволяет ускорить проверку частных прав доступа.

В кэше прав доступа может храниться не более 32 частных прав доступа к объектам и не более 32 частных прав доступа к спискам прав доступа. Кэш обновляется в момент предоставления прав доступа пользователю и при аннулировании прав доступа. Все пользовательские кэши очищаются во время выполнения IPL.

Хотя широко применять частные права доступа по-прежнему не рекомендуется, кэш частично сглаживает недостатки их использования. В частности, при выборе способа защиты объектов можно меньше внимания уделять его влиянию на производительность системы. Больше всего это проявляется в тех случаях, когда пользователи многократно обращаются к одним и тем же объектам.

Глава 6. Защита управления заданиями

В этом разделе приведена информация о защите средств управления заданиями в системе.

Далее рассмотрены следующие вопросы.

Информация, связанная с данной

Управление работой

Инициализация задания

При запуске задания система проверяет права доступа к некоторым объектам.

При запуске задания система связывает с ним ряд объектов, в том числе очередь вывода, описание задания и библиотеки из списка библиотек. Права доступа к некоторым из этих объектов проверяются еще до запуска задания, а права доступа к остальным объектам - уже после запуска. Отсутствие необходимых прав доступа может привести к возникновению ошибок или завершению работы задания.

Входящие в состав структуры задания объекты могут быть заданы в описании задания, в пользовательском профайле, а в случае пакетного задания - в команде Передать задание на выполнение (SBMJOB).

Запуск интерактивного задания

Ниже описаны действия по защите, выполняемые во время запуска интерактивного задания.

Поскольку используемые заданием объекты можно задавать различными способами, это описание следует рассматривать только как пример.

Если во время входа в систему возникает ошибка, связанная с правами доступа, то в нижней области меню Вход в систему появляется сообщение об ошибке. При возникновении некоторых подобных ошибок создается протокол задания. Если пользователю был запрещен вход в систему из-за ошибки, связанной с правами доступа, то следует задать другой объект в пользовательском профайле или предоставить пользователю права доступа к текущему объекту.

В промежутке между вводом имени и пароля пользователя и запуском задания в системе выполняются следующие действия:

1. Проверяются пользовательский профайл и пароль. Пользовательский профайл должен находиться в состоянии *ENABLED. Кроме того, пользовательскому профайлу, указанному в меню входа в систему, должны быть предоставлены права доступа *OBJOPR, а также права доступа *CHANGE по отношению к самому себе.
2. Проверяются права пользователя на использование рабочей станции. Дополнительная информация приведена в разделе “Рабочие станции” на стр. 211.
3. Система проверяет права доступа к объектам, заданным в пользовательском профайле и описании задания пользователя и применяемым для создания структуры задания. В их число входят:
 - Описание задания
 - Очереди вывода
 - Текущая библиотека
 - Библиотеки из списка библиотек

Если какие-либо из этих объектов не существуют, либо пользователю не предоставлены необходимые права доступа к этим объектам, то в нижней области меню Вход в систему появится сообщение об ошибке, а пользователю будет запрещен вход в систему. Если проверка прав доступа к этим объектам завершится успешно, то задание будет запущено в системе.

Примечание: Права доступа к принтеру и очереди задания проверяются только при обращении к этим объектам.

В промежутке между запуском задания и появлением первого меню выполняются следующие действия:

1. Если в записи о выполнении задания указана пользовательская программа, то выполняется обычная процедура проверки прав доступа к программе, библиотеке программы и объектам, используемым в программе. Если необходимые права доступа не предоставлены, то в меню Вход в систему появляется соответствующее сообщение, а выполнение задания завершается.
2. Если в записи о выполнении задан командный процессор (QCMD):
 - a. Выполняется проверка прав доступа к программе QCMD, библиотеке этой программы и используемым объектам, как описано на шаге 1.
 - b. Проверяется наличие прав доступа к программе обработки нажатия клавиши Attention и ее библиотеке. Если необходимые права доступа не предоставлены, то создается сообщение, которое отправляется пользователю и записывается в протокол задания. Обработка продолжается. Если необходимые права доступа предоставлены, то программа обработки нажатия клавиши Attention активируется. Запуск программы выполняется только при первом нажатии клавиши Attention. В этот момент выполняется обычная процедура проверки прав доступа к объектам, применяемым программой.
 - c. Выполняется обычная проверка наличия прав доступа к начальной программе, указанной в пользовательском профайле, и связанным с ней объектам. При наличии необходимых прав доступа программа запускается. Если необходимые права доступа не предоставлены, то создается сообщение, которое отправляется пользователю и записывается в протокол задания. Выполнение задания завершается.
 - d. Выполняется обычная проверка наличия прав доступа к начальному меню, указанному в пользовательском профайле, и связанным с ним объектам. Если необходимые права доступа предоставлены, то отображается начальное меню. Если необходимые права доступа не предоставлены, то создается сообщение, которое отправляется пользователю и записывается в протокол задания. Выполнение задания завершается.

Запуск пакетного задания

В этом разделе описаны действия по защите, выполняемые во время запуска пакетного задания.

Поскольку передавать задание на выполнение и указывать используемые заданием объекты можно различными способами, это описание следует рассматривать только как пример. В примере рассматривается задание, переданное на выполнение из интерактивного задания с помощью команды SBMJOB.

В промежутке между запуском команды SBMJOB и добавлением задания в очередь заданий выполняется следующая проверка:

1. Если в команде SBMJOB был задан пользовательский профайл, то вам должны быть предоставлены права доступа *USE к этому пользовательскому профайлу.
2. Проверяется наличие прав доступа к объектам, указанным в параметрах команды SBMJOB и в описании задания. Эти права доступа должны быть предоставлены пользовательскому профайлу, под управлением которого будет выполняться задание.
3. Если уровень защиты равен 40 или 50, и в команде SBMJOB был задан параметр USER(*JOBID), то запустившему заданию пользователю должны быть предоставлены права доступа *USE по отношению к пользовательскому профайлу, заданному в описании задания.
4. При обнаружении несуществующего объекта или отсутствии необходимых прав доступа пользователю отправляется сообщение, а выполнение задания завершается.

При запуске задания из очереди заданий выполняется такая процедура проверки, как при запуске интерактивного задания.

Принятые права доступа и пакетные задания

Параметры пакетного задания, работающего с принятыми правами доступа, можно изменить.

При запуске задания создается стек вызовов для этого задания. Принятые права доступа вступают в силу только после добавления первой программы в стек. Принятые права доступа не могут применяться для получения доступа к объектам из структуры задания, таким как очередь вывода и описание задания, пока не был начат шаг выполнения. Это означает, что если в момент передачи задания на выполнение интерактивное задание применяло принятые права доступа, эти права доступа не будут использоваться при проверке прав доступа к объектам, указанным в команде SBMJOB.

В то время, когда пакетное задание ожидает запуска, его свойства можно изменить с помощью команды Изменить задание (CHGJOB). Права доступа, необходимые для изменения параметров задания, указаны в разделе Команды заданий.

Рабочие станции

При входе в систему проверяются права доступа для рабочей станции.

Описание устройства содержит информацию о физическом или логическом устройстве, подключенном к системе. В момент входа в систему рабочая станция подключена к описанию физического или виртуального устройства. Для успешного входа в систему необходимы права доступа *CHANGE к этому описанию устройства.

Системное значение QLMTSECOFR (Ограничить права системного администратора) указывает, нужно ли явно предоставлять права доступа к описаниям устройств пользователям со специальными правами доступа *ALLOBJ или *SERVICE.

На рис. 28 на стр. 212 приведена блок-схема, в соответствии с которой пользователю разрешается или запрещается вход в систему с устройства:

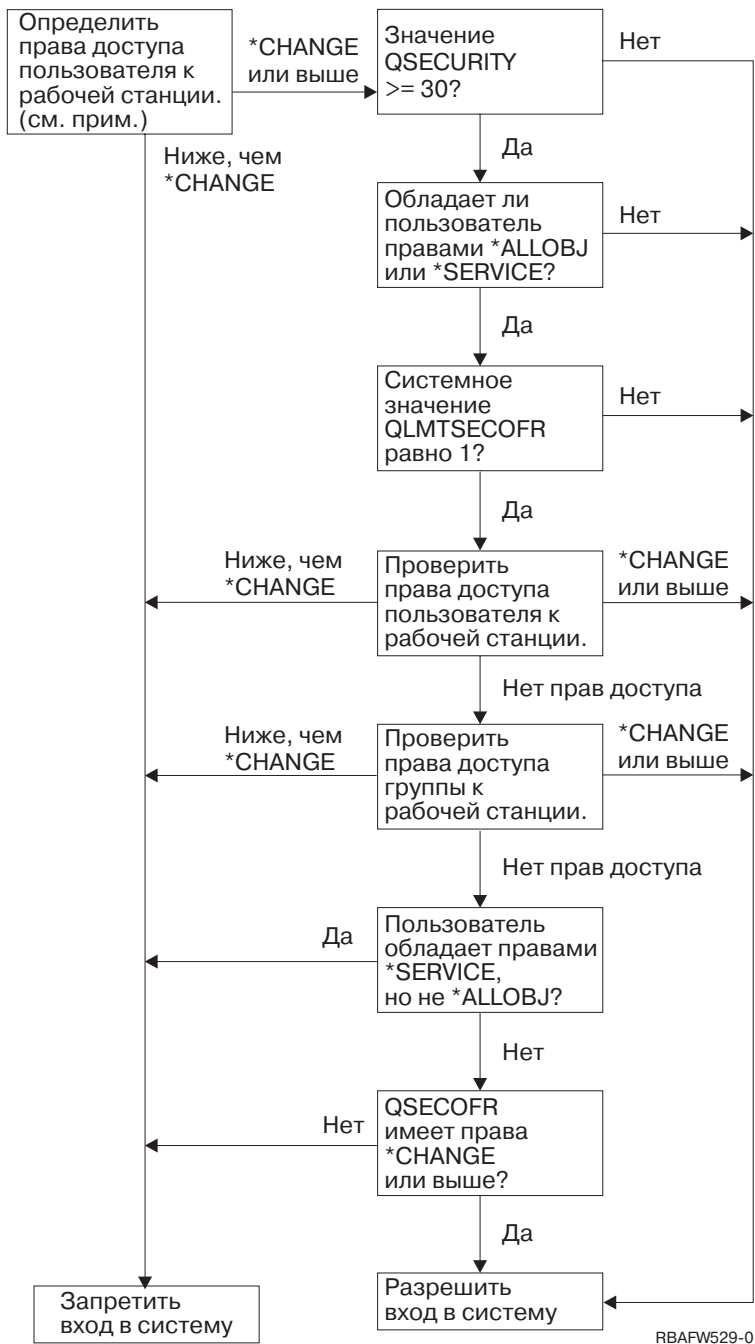


Рисунок 28. Проверка прав доступа для рабочей станции

Примечание: Для проверки наличия прав доступа *CHANGE к описанию устройства выполняется обычная процедура проверки прав доступа. Права доступа *CHANGE могут быть предоставлены одним из следующих способов:

- Как составная часть специальных прав доступа *ALLOBJ, предоставленных пользовательскому профайлу, профайлу основной группы или профайлу дополнительной группы.
- Как частные права доступа к описанию устройства, предоставленные пользовательскому профайлу, профайлу основной группы или профайлу дополнительной группы.
- Как права доступа к списку прав доступа, применяемому для защиты описания устройства.
- Как права доступа к списку прав доступа, определяющему общие права доступа.

Проверка прав доступа к описанию устройства выполняется до помещения каких-либо программ в стек вызова задания, поэтому принятые права доступа не учитываются.

Описание процедуры проверки прав доступа к рабочим станциям

Система проверяет наличие у пользователя прав доступа к рабочей станции. (См. примечание 1) Если пользователю предоставлены права доступа более низкого уровня, чем *CHANGE, то вход в систему запрещается. Если пользователю предоставлены права доступа *CHANGE или выше, то система выясняет, чему равен текущий уровень защиты. Если уровень защиты меньше 30, то пользователю разрешается вход в систему.

Если уровень защиты равен 30 или выше, то система проверяет наличие специальных прав доступа *ALLOBJ или *SERVICE. Если пользователю не предоставлены ни одни из этих специальных прав доступа, то вход в систему разрешается.

Если пользователю предоставлены специальные права доступа *ALLOBJ или *SERVICE, то система проверяет, чему равно системное значение QLMTSECOFR. Если оно не равно 1, то вход в систему разрешается.

Если системное значение QLMTSECOFR равно 1, то система проверяет права доступа пользователя к рабочей станции. Если пользователю предоставлены права доступа *CHANGE или права доступа более высокого уровня, то вход в систему разрешается. Если пользователю предоставлены права доступа более низкого уровня, то вход в систему запрещается. Если пользователю не предоставлены никакие права доступа к рабочей станции, то система проверяет права доступа его группы.

Если группе пользователя предоставлены права доступа *CHANGE или права доступа более высокого уровня, то вход в систему разрешается. Если группе предоставлены права доступа более низкого уровня, то вход в систему запрещается. Если группе пользователя не предоставлены никакие права доступа к рабочей станции, то система проверяет, не предоставлены ли пользователю специальные права доступа *SERVICE без специальных прав доступа *ALLOBJ.

Если пользователю предоставлены специальные права доступа *SERVICE, и не предоставлены права доступа *ALLOBJ, то вход в систему запрещается. Если пользователю предоставлены права доступа *ALLOBJ, то система проверяет, предоставлены ли пользователю QSECOFR права доступа *CHANGE или права доступа более высокого уровня.

Если QSECOFR не предоставлены права доступа *CHANGE или права более высокого уровня, то вход в систему запрещается. Если QSECOFR предоставлены права доступа *CHANGE или права более высокого уровня, то вход в систему разрешается.

Пользовательскому профайлу системного администратора (QSECOFR), служебному пользовательскому профайлу (QSRV) и основному служебному пользовательскому профайлу (QSRVBAS) всегда разрешается вход в систему с консоли. Устройство, играющее роль консоли, определяется с помощью системного значения QCONSOLE. Если профайл QSRV или QSRVBAS попытается войти в систему с консоли, и у него не будет прав доступа *CHANGE, то система предоставит ему права доступа *CHANGE и разрешит вход в систему.

Принадлежность описаний устройств

Принадлежность описаний устройств позволяет управлять правами доступа к устройствам.

По умолчанию команда CRTDEVxxx устанавливает общие права доступа *CHANGE. Устройства создаются в библиотеке QSYS, которая поставляется с параметром CRTAUT, равным *SYSVAL. Системное значение QCRTAUT поставляется со значением *CHANGE.

Для того чтобы ограничить круг пользователей, которым разрешено входить в систему с рабочей станции, измените общие права доступа к рабочей станции на *EXCLUDE и предоставьте права доступа *CHANGE отдельным пользователям и группам.

Системному администратору (QSECOFR) не предоставлены права доступа к отдельным устройствам. Если системное значение QLMTSECOFR равно 1 (Да), то системному администратору необходимо явно предоставить права доступа *CHANGE по отношению к устройствам. Любой пользователь, которому предоставлены права доступа *OBJMGT и *CHANGE по отношению к устройству, может предоставить права доступа *CHANGE другому пользователю (в том числе и системному администратору).

Если описание устройства было создано системным администратором, то системный администратор является владельцем устройства, и ему предоставлены права доступа *ALL по отношению к нему. Если устройства настраивались автоматически, то большинство устройств будут принадлежать профайлу QPGMR. Устройства, созданные программой QLUS (устройства типа *APPC), принадлежат профайлу QSYS.

Если с помощью системного значения QLMTSECOFR вы планируете ограничить набор устройств, с которых разрешено входить в систему системному администратору, то владельцем всех создаваемых устройств следует назначать профайл, отличный от QSECOFR.

Для изменения принадлежности описания дисплейного устройства необходимо включить питание устройства и активировать его. Войдите в систему с дисплейного устройства и измените принадлежность с помощью команды CHGOBJOWN. Если вы вошли в систему с другого устройства, то для изменения принадлежности дисплейного устройства его необходимо предварительно захватить с помощью команды Захватить объект (ALCOBJ). Устройство можно захватить только в том случае, если оно не занято. После изменения принадлежности освободите устройство с помощью команды Освободить объект (DLCOBJ).

Файл меню входа в систему

Системный администратор может изменить меню входа в систему. Например, можно добавить в меню текст или эмблему компании.

При добавлении текста в файл меню входа в систему следует следить за тем, чтобы имена полей и длины буферов оставались прежними. Изменение имени поля или длины буфера может привести к сбою при входе в систему.

Изменение меню входа в систему

Исходный код в файле меню входа в систему можно изменить, чтобы изменить меню входа в систему.

Исходный код меню входа в систему поставляется вместе с операционной системой. Он расположен в файле QSYS/QAWTSSRC. Вы можете добавить текст в меню входа в систему, изменив исходный код. При этом следует сохранять имена полей и длины буферов.

Исходный код меню входа в систему

Для создания собственного меню входа в систему требуется скопировать соответствующий исходный файл.

Исходный код меню входа в систему поставляется как элемент QDSIGNON или QDSIGNON2 физического файла QSYS/QAWTSSRC. Элемент QDSIGNON содержит исходный код меню входа в систему, применяемого в том случае, если системное значение QPWDLVL равно 0 или 1. Элемент QDSIGNON2 содержит исходный код меню входа в систему, применяемого в том случае, если системное значение QPWDLVL равно 2 или 3.

Файл QSYS/QAWTSSRC удаляется и восстанавливается при каждой установке операционной системы i5/OS. Если вы планируете создать свой вариант меню входа в систему, то скопируйте элемент исходного файла (QDSIGNON или QDSIGNON2) в собственный исходный файл и внесите изменения в этой копии файла.

Изменение файла меню входа в систему

В этом разделе описано, как изменить файл меню входа в систему.

Для изменения формата меню входа в систему выполните следующие действия:

1. Создайте новый файл меню входа в систему.

Вы можете изменить скрытое поле файла меню UBUFFER для работы с более мелкими полями. Длина поля UBUFFER составляет 128 байт. Это поле является последним полем файла меню. Вы можете изменить это поле таким образом, чтобы оно играло роль буфера ввода-вывода. Тогда указанные в этом поле данные будут доступны прикладным программам, запущенным интерактивным заданием. Поле UBUFFER можно изменить таким образом, чтобы оно содержало любое число полей меньшего размера, если выполнены следующие условия:

- Новые поля должны быть расположены после всех остальных полей в файле меню. Расположение полей в меню не имеет значения, в то время как расположение данных в спецификации описания данных (DDS) важно.
- Общая длина полей должна составлять 128 байт. Если длина полей превышает 128, то некоторые данные могут быть потеряны.
- Все поля должны являться полями ввода-вывода (поля типа В в исходном тексте DDS) или скрытыми полями (поля типа Н в исходном тексте DDS).

2. Порядок объявления полей в файле меню входа в систему должен остаться прежним. Расположение этих полей в меню может быть изменено. Не изменяйте имена существующих полей в исходном тексте файла меню входа в систему.

3. Не изменяйте общий размер буферов ввода или вывода. Изменение размера или порядка буферов может привести к возникновению серьезных неполадок.

4. Не используйте функцию справки, предусмотренную в спецификациях описания данных (DDS), в файле меню входа в систему.

5. Замените файл по умолчанию QSYS/QDSIGNON на новый файл меню в описании подсистемы. Измените те описания подсистем, которые должны применять новое меню. Для изменения описания подсистемы выполните следующие действия:

- а. Введите команду Изменить описание подсистемы (CHGSBSD).
- б. Укажите новый файл меню в параметре SGNDSPF.
- в. Используя тестовую версию подсистемы, проверьте правильность меню. После этого измените управляющую подсистему.

6. Протестируйте внесенное изменение.

7. Измените остальные описания подсистем.

Notes:

1. Длина буфера в файле меню должна составлять 318 байт. Если длина буфера будет меньше этого значения, то подсистема покажет меню входа в систему по умолчанию, то есть элемент QDSIGNON из библиотеки QSYS, если системное значение QPWLVL равно 0 или 1, либо элемент QDSIGNON2 из библиотеки QSYS, если системное значение равно QPWLVL 2 или 3.
2. Не следует удалять информацию об авторских правах.

Описания подсистем

Описания подсистем применяются для различных функций в системе.

Описания подсистем управляют следующими аспектами работы заданий:

- Способом входа заданий в систему
- Способом запуска заданий
- Параметрами производительности заданий

Права на изменение описаний подсистем следует предоставить только узкому кругу пользователей. Все вносимые изменения следует тщательно отслеживать.

Понятия, связанные с данным

“Вход в систему без ИД пользователя и пароля” на стр. 17

Способ входа в систему без ИД пользователя и пароля определяется на основе уровня защиты.

Управление передачей новых заданий в систему

Описания подсистем можно использовать для управления передачей новых заданий в систему.

Вместе с системой поставляется несколько описаний подсистем. Если вы измените уровень защиты (системное значение QSECURITY) на уровень 20 или более высокий уровень, то для входа в систему с помощью поставляемых фирмой IBM подсистем будет требоваться вводить имя и пароль пользователя.

Однако всегда можно определить такие описание подсистемы и описание задания, которые будут применять опцию входа в систему по умолчанию (без ввода имени и пароля пользователя). Это представляет потенциальную угрозу для защиты системы. Когда система передает на выполнение интерактивное задание, то она выполняет поиск описания задания в записи рабочей станции, указанной в описании подсистемы. Если в описании задания задан параметр USER(*RQD), то пользователю потребуется ввести правильные имя и пароль в меню входа в систему. Если в поле *Пользователь* описания задания задан пользовательский профайл, то любой пользователь может нажать клавишу Enter и войти в систему с использованием этого профайла.

Если установлен уровень защиты 30 или выше и включена функция контроля, то система добавляет в журнал контроля записи обо всех попытках входа в систему с профайлом по умолчанию (запись типа AF, подтип S). Если установлен уровень защиты 40 или выше, то система запрещает вход в систему с профайлом по умолчанию, даже если есть описание задания и запись рабочей станции, позволяющие это сделать. Дополнительная информация приведена в разделе “Вход в систему без ИД пользователя и пароля” на стр. 17.

Убедитесь, что во всех записях рабочих станций из описаний интерактивных подсистем заданы описания заданий с параметром USER(*RQD). Ограничьте права на изменение описаний заданий и отслеживайте все подобные изменения. Если включена функция контроля, то система создает записи журнала типа JD обо всех операциях изменения параметра USER в описании задания.

Записи средств связи из описания подсистемы определяют способ входа заданий связи в систему. Запись средств связи задает пользовательский профайл по умолчанию, позволяющий запустить задание без ввода имени и пароля пользователя. Потенциально это позволяет обойти защиту. Проверьте записи средств связи в системе и настройте способ входа заданий связи в систему с помощью сетевых атрибутов. В разделе “Атрибуты сети” на стр. 225 описаны важные с точки зрения защиты сетевые атрибуты.

Описания заданий

Описание задания - это мощный инструмент управления защитой и заданиями.

Описание задания можно настроить для группы пользователей, которые должны применять одинаковый начальный список библиотек, очередь вывода и очередь заданий. Кроме того, описание задания можно настроить для группы пакетных заданий с одинаковыми требованиями.

В то же время, описание задания теоретически может использоваться для обхода защиты. В некоторых случаях описание задания, содержащее имя профайла в параметре USER, позволяет заданию войти в систему без проверки идентификационной информации. В разделе “Управление передачей новых заданий в систему” приведена информация о том, как закрыть эту брешь в защите для интерактивных заданий и заданий связи.

Пакетное задание не обязательно выполняется с тем профайлом, который связан с пользователем, запустившим это задание. Необходимый профайл можно указать в команде SBMJOB или в параметре USER описания задания. Если в системе установлен уровень защиты 30 или более низкий уровень (он определяется системным значением QSECURITY), то для передачи задания на выполнение пользователю необходимы права доступа к описанию задания, но не к пользовательскому профайлу, указанному в описании задания. В некоторых случаях это позволяет обойти защиту. Если уровень защиты не ниже 40, то для передачи задания на выполнение необходимы права доступа как к описанию задания, так и к указанному в нем пользовательскому профайлу.

Например:

- Пользователю USERA не предоставлены права доступа к файлу PAYROLL.
- Пользователю USERB предоставлены права доступа *USE по отношению к файлу PAYROLL и программе PRLIST, которая показывает содержимое файла PAYROLL.
- В описании задания PRJOBД задан параметр USER(USERB). Общие права доступа к описанию PRJOBД равны *USE.

Если уровень защиты не выше 30, то пользователь USERA может просмотреть файл PAYROLL, передав на выполнение следующее пакетное задание:

```
SBMJOB RQSDTA("Call PRLIST") JOBД(PRJOBД) +  
USER(*JOBД)
```

Для того чтобы предотвратить эту ситуацию, следует установить уровень защиты не ниже 40 или ограничить права доступа к описаниям заданий, в которых задан пользовательский профайл.

Для выполнения некоторых типов пакетных заданий требуется, чтобы в описании задания было задано имя пользовательского профайла. Например, описание задания QWATCH поставляется с параметром USER(QPGMR). Поставляемые общие права доступа к этому описанию равны *EXCLUDE.

Если в системе установлен уровень защиты не выше 30, то любой пользователь, которому предоставлены права доступа к команде Передать задание на выполнение (SBMJOB) или командам запуска программы чтения и права доступа *USE к описанию задания QWATCH, может передавать задания на выполнение с использованием пользовательского профайла программиста (QPGMR), независимо от наличия прав доступа к этому профайлу. Если установлен уровень защиты не ниже 40, то для этого требуются права доступа *USE к профайлу QPGMR.

Очередь сообщений системного оператора

В этом разделе описаны права доступа для очереди сообщений системного оператора.

В меню Операционная поддержка i5/OS (ASSIST) предусмотрена опция для управления системой, пользователями и устройствами. В меню Управление системой, пользователями и устройствами предусмотрена опция для работы с сообщениями из очереди системного оператора. В некоторых случаях имеет смысл запретить пользователям отвечать на сообщения из очереди системного оператора (QSYSOPR). Выбор неправильного ответа на подобное сообщение может привести к возникновению неполадок в системе.

Для отправки ответов на сообщения необходимы права доступа *USE и *ADD по отношению к очереди сообщений. Для удаления сообщений необходимы права доступа *USE и *DLT, см. раздел Команды для работы с сообщениями. Права доступа на удаление сообщений из QSYSOPR и отправку ответов на эти сообщения следует предоставлять только пользователям, выполняющим функции системного оператора. Набор общих прав доступа к QSYSOPR должен состоять из прав *OBJOPR и *ADD, чтобы любые пользователи могли добавлять сообщения в QSYSOPR.

Внимание: У всех заданий должна быть возможность добавлять сообщения в очередь QSYSOPR. Не устанавливайте общие права доступа *EXCLUDE для QSYSOPR.

Списки библиотек

Список библиотек задания определяет набор библиотек, просматриваемых при поиске, и порядок просмотра библиотек.

Объекты в программе могут указываться с помощью полного имени, состоящего из имени объекта и имени библиотеки. Также в качестве библиотеки объекта может быть задано значение *LIBL (список библиотек). В этом случае библиотеки из списка будут просматриваться в указанном порядке до обнаружения первого совпадения.

В Табл. 123 приведен обзор фрагментов списка библиотек и процедуры их выбора в задании. Риски, связанные с применением библиотек, и необходимые меры по защите описаны в следующих разделах.

Таблица 123. Компоненты списка библиотек. Во время поиска компоненты списка библиотек перебираются в следующей последовательности:

Компонент	Способ определения значения
15 записей системной части	Начальное значение считывается из системного значения QSYSLIBL. Во время выполнения задания его можно изменить с помощью команды CHGSYSLIBL.
Часть 2 (рабочие библиотеки)	Вначале список пуст. Библиотека добавляется в перечень рабочих библиотек из списка библиотек при запуске команды или меню, в параметре PRDLIB которой было задано имя библиотеки. Имя библиотеки хранится в перечне рабочих библиотек до завершения работы с командой или меню.
Запись о текущей библиотеке	Указывается в пользовательском профайле или в меню входа в систему. Эта запись изменяется при запуске команды или меню, в параметре CURLIB которых задано имя библиотеки. Данное значение можно изменить во время выполнения задания с помощью команды CHGCURLIB.
250 записей пользовательской части	В качестве начального значения применяется начальный список библиотек из описания задания пользователя. Если в описании задания указано значение *SYSVAL, то применяется системное значение QURLIBL. В процессе выполнения задания пользовательскую часть списка библиотек можно изменить с помощью команд ADDLIBL, RMVLIBL, CHGLIBL и EDTLIBL.

Понятия, связанные с данным

“Защита библиотек и списки библиотек” на стр. 142

При добавлении библиотеки в список библиотек пользователя права доступа пользователя к библиотеке сохраняются вместе со списком.

“Планирование библиотек” на стр. 236

Структура библиотеки аналогична структуре каталога, позволяющего искать размещенные в нем объекты. Способ объединения информации приложения в библиотеки и управления библиотеками зависит от большого числа факторов.

Риски, связанные с применением списков библиотек

В данном разделе описаны примеры обхода защиты при работе со списками библиотек и меры по его предотвращению.

Списки библиотек потенциально предоставляют возможность обойти защиту. Имея возможность изменять последовательность библиотек в списке или добавлять новые библиотеки в список, пользователь может выполнять функции, противоречащие требованиям защиты.

В разделе “Защита библиотек и списки библиотек” на стр. 142 приведена общая информация о возможных проблемах, связанных со списками библиотек.

Ниже приведены два примера обхода защиты путем изменения списка библиотек.

Изменения в функции

В этом примере описан возможный риск изменения функции при вызове программы библиотеки.

На рис. 29 показана библиотека приложения. Программа А вызывает программу В, которая должна располагаться в библиотеке LIBA. Программа В обновляет файл А. В вызове программы В ее имя указано без имени библиотеки, поэтому для поиска программы В применяется список библиотек.

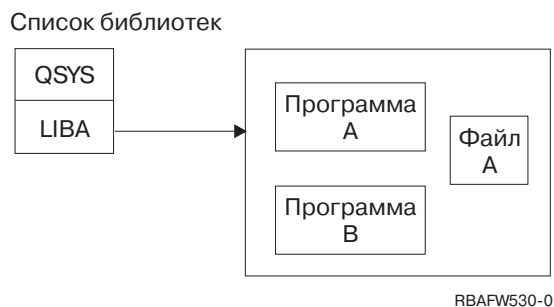


Рисунок 29. Список библиотек – ожидаемая среда

Программист или другой хорошо осведомленный пользователь может поместить другую программу В в библиотеку LIBB. Эта программа может выполнять совсем другие действия, например копировать конфиденциальную информацию или вносить неправильные изменения в файлы. Если библиотека LIBB будет помещена в список библиотек перед библиотекой LIBA, то вместо настоящей программы В будет вызвана замещающая ее программа, так как имя программы В указано без имени библиотеки:

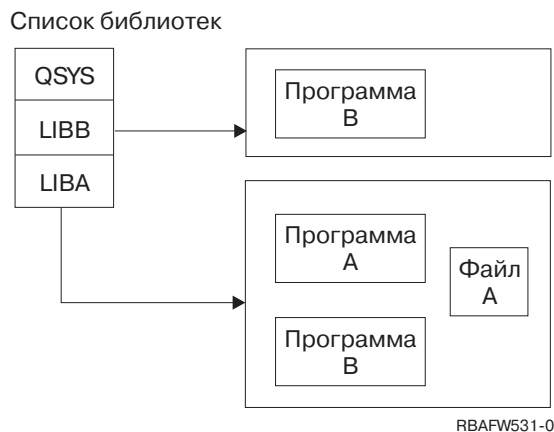


Рисунок 30. Список библиотек – фактическая среда

Несанкционированный доступ к информации

Этот пример иллюстрирует потенциальную опасность несанкционированного доступа к информации в библиотеке.

Предположим, что программа А из примера рис. 29 принимает права доступа пользователя USER1, которому предоставлены права доступа *ALL к файлу А (при этом принятые права доступа продолжают действовать). Любой хорошо осведомленный пользователь может создать замещающую программу В, вызывающую командный процессор. В этом случае пользователь получит доступ к командной строке и все права доступа к файлу А.

Рекомендации по настройке системной части списка библиотек

В этом разделе приведены рекомендации для системной части списка библиотек.

В системной части списка библиотек располагаются поставляемые фирмой IBM библиотеки. Дополнительно в эту часть списка библиотек можно поместить библиотеки приложений, если доступ к ним ограничен соответствующим образом. При этом риск будет максимальным, так как библиотеки из системной части списка первыми просматриваются при поиске.

Системное значение QSYSLIBL разрешено изменять только пользователям со специальными правами *ALLOBJ и *SECADM. Необходимо контролировать и отслеживать все изменения, которые вносятся в системную часть списка библиотек. Ниже приведены некоторые рекомендации по добавлению библиотек:

- В эту часть списка библиотек следует добавлять только те библиотеки, права доступа к которым настраиваются индивидуально.
- Общие права доступа к этим библиотекам не должны равняться *ADD.
- Для работы с некоторыми поставляемыми фирмой IBM библиотеками необходимо, чтобы общие права доступа к ним были равны *ADD (это поставляемое значение). Регулярно проверяйте, какие объекты были добавлены в эти библиотеки. Особое внимание следует обращать на программы, исходные файлы и команды.

Команда CHGSYSLIBL поставляется с общими правами доступа *EXCLUDE. По умолчанию доступ к этой команде предоставлен только пользователям с правами доступа *ALLOBJ. Для изменения системной части списка библиотек на время выполнения задания можно воспользоваться способом, описанным в разделе “Изменение списка системных библиотек” на стр. 239.

Рекомендации по настройке рабочей библиотеки

В этом разделе приведены рекомендации по защите рабочей библиотеки.

Та часть списка библиотек, в которой перечислены рабочие библиотеки, во время поиска просматривается перед пользовательской частью списка. Осведомленный об этом пользователь может создать команду или меню для добавления рабочей библиотеки в список библиотек. Например, следующий оператор создает команду CMDX, запускающую программу PGMA:

```
CRTCMD CMDX PGM(PGMA) PRDLIB(LIBB)
```

Во время выполнения CMDX среди других рабочих библиотек из списка библиотек будет находиться библиотека LIBB.

Ниже перечислены рекомендуемые меры по защите той части списка библиотек, которая содержит рабочие библиотеки:

- Ограничьте доступ к командам Создать команду (CRTCMD), Изменить команду (CHGCMD), Создать меню (CRTMNU) и Изменить меню (CHGMNU).
- При создании команд и меню указывайте параметр PRDLIB(*NONE), чтобы из рабочей части списка библиотек были удалены все записи. Это позволяет предотвратить просмотр неизвестных библиотек перед ожидаемой библиотекой во время поиска при выполнении команды или меню.

Примечание: По умолчанию при создании команды или меню применяется параметр PRDLIB(*NOCHG). *NOCHG означает, что при выполнении команды или меню рабочие библиотеки из списка библиотек не изменяются.

Рекомендации по настройке текущей библиотеки

В этом разделе приведены рекомендации по защите системы при работе с текущей библиотекой.

Текущая библиотека применяется средствами поддержки принятия решений, такими как Query/400. Все создаваемые пользователем программы обработки запросов по умолчанию размещаются в текущей библиотеке этого пользователя. При создании меню или команды можно указать текущую библиотеку, которая будет применяться при работе с меню.

Текущая библиотека позволяет пользователям и программистам не задумываться о том, где следует размещать созданные объекты, такие как программы обработки запросов. Однако потенциально текущая библиотека позволяет обойти защиту, так как она просматривается раньше пользовательской части списка библиотек во время поиска. Для того чтобы предотвратить такой обход защиты, сохранив возможность использования текущей библиотеки, рекомендуется принять следующие меры предосторожности:

- Укажите значение *YES в поле *Ограничить возможности* пользовательского профайла. В результате пользователю будет запрещено изменять текущую библиотеку с помощью меню входа в систему или команды CHGPRF.
- Ограничьте права доступа к командам Изменить текущую библиотеку (CHGCURLIB), Создать меню (CRTMNU), Изменить меню (CHGMNU), Создать команду (CRTCMD) и Изменить команду (CHGCMD).
- Для настройки текущей библиотеки во время выполнения приложения следуйте инструкциям, приведенным в разделе “Управление списком пользовательских библиотек” на стр. 238.

Рекомендации по настройке пользовательской части списка библиотек

В этом разделе приведены рекомендации по настройке пользовательской части списка библиотек.

Как правило, пользовательская часть списка библиотек изменяется чаще, чем другие компоненты списка библиотек, поэтому ее сложнее контролировать. Список библиотек изменяют многие приложения. Список библиотек заданий определяется описаниями этих заданий.

Ниже приведено несколько возможных способов управления пользовательской частью списка библиотек, позволяющих предотвратить применение запрещенных библиотек с замещающими программами и файлами во время выполнения:

- Ограничьте возможности пользователей рабочих приложений возможностями меню. Для того чтобы запретить пользователям вводить команды, укажите значение *YES в поле *Ограничить возможности* пользовательских профайлов. В разделе “Планирование меню” на стр. 240 приведен пример такой среды.
- Указывайте в приложениях полные имена (имя объекта и имя библиотеки). Это позволит избежать необходимости выполнять поиск объекта в списке библиотек.
- Ограничьте права на изменение описаний заданий, так как описание задания определяет начальный список библиотек задания.
- Добавляйте библиотеку, содержащую необходимые объекты, в начало пользовательской части списка библиотек, используя команду Добавить запись списка библиотек (ADDLIBLE) в начале программы. Добавленную библиотеку можно удалить в конце программы.

Если библиотека уже есть в списке, но вы не уверены, что она находится в начале списка, то удалите эту библиотеку, а затем добавьте ее снова. Если порядок библиотек в списке важен для других приложений системы, то вместо этого способа используйте указанный ниже.

- Воспользуйтесь программой, которая получает и сохраняет список библиотек задания. С ее помощью замените текущий список библиотек на тот список, который подходит для приложения. При завершении работы приложения восстановите исходный список библиотек. Пример выполнения этой процедуры приведен в разделе “Управление списком пользовательских библиотек” на стр. 238.

Печать

В этом разделе описано управление защитой очередей вывода в системе.

Обычно отправленная на печать информация сохраняется в буферном файле и помещается в очередь вывода на то время, пока она ожидает освобождения принтера. Если вы не обеспечите защиту очередей вывода в системе, то злоумышленники смогут просматривать, печатать и копировать конфиденциальную информацию, ожидающую печати.

Один из возможных способов защиты конфиденциального вывода заключается в создании особой очереди вывода. Всю конфиденциальную информацию можно отправлять в одну очередь вывода, предварительно ограничив права на просмотр буферных файлов из этой очереди и работу с ними.

Для того чтобы определить, в какую очередь вывода следует направить информацию, система последовательно проверяет значения из файла принтера, атрибутов задания, пользовательского профайла, описания устройства рабочей станции и системного значения Принтер (QPRTDEV). По умолчанию применяется очередь вывода, связанная с принтером QPRTDEV. Примеры отправки вывода в конкретную очередь вывода приведены в разделе Расширенная презентация функции.

Защита буферных файлов

В этом разделе описаны параметры, применяемые для защиты буферных файлов.

Буферный файл - это особый тип объектов в системе. Вы не можете явно настроить права на просмотр и права на работу с буферным файлом. Права доступа к буферному файлу определяются несколькими параметрами той очереди вывода, в которой расположен буферный файл.

Вначале владельцем буферного файла назначается тот пользователь, который его создал. Владелец буферного файла всегда разрешено просматривать этот файл и работать с ним, независимо от того, какие права доступа определены для очереди вывода. Для добавления записей в очередь вывода необходимы права доступа *READ. Даже если пользователю запрещен доступ к очереди вывода, он может работать с принадлежащими ему записями из очереди с помощью команды Работа с буферными файлами (WRKSPLF).

Параметры защиты очереди вывода настраиваются с помощью команд Создать очередь вывода (CRTOUTQ) и Изменить очередь вывода (CHGOUTQ). Эти параметры можно просмотреть с помощью команды Работа с описанием очереди вывода (WRKOUTQD).

Внимание: Пользователь со специальными правами доступа *SPLCTL может выполнять любые функции над любыми записями, независимо от параметров очереди вывода. Некоторые параметры очереди вывода позволяют пользователю со специальными правами доступа *JOBCTL просматривать содержимое записей очереди вывода.

Параметр очереди вывода Показать данные (DSPDTA)

Параметр Показать данные (DSPDTA) предназначен для защиты содержимого буферного файла.

Параметр DSPDTA определяет, какие права доступа необходимы для выполнения указанных ниже функций над буферными файлами, принадлежащими другим пользователям:

- Просмотреть содержимое буферного файла (команда DSPSPLF)
- Скопировать буферный файл (команда CPYSPLF)
- Отправить буферный файл (команда SNDNETSPLF)
- Переместить буферный файл в другую очередь вывода (команда CHGSPLFA)

Возможные значения параметра DSPDTA	
*NO	Пользователю запрещено просматривать, отправлять и копировать буферные файлы, принадлежащие другим пользователям, если у него нет каких-либо из следующих прав доступа: <ul style="list-style-type: none"> • Специальных прав доступа *JOBCTL, если параметр OPRCTL равен *YES. • Прав доступа *READ, *ADD и *DLT по отношению к очереди вывода, если параметр *AUTCHK равен *DTAAUT. • Прав владельца очереди вывода, если параметр *AUTCHK равен *OWNER.
*YES	Любой пользователь с правами доступа *READ к очереди вывода может просматривать, копировать и отправлять данные буферных файлов, принадлежащих другим пользователям.

<i>Возможные значения параметра DSPDTA</i>	
*OWNER	Просматривать, копировать, отправлять и перемещать буферный файл разрешено только его владельцу и пользователям с правами доступа *SPLCTL (управление буфером). Если параметр OPRCTL равен *YES, то пользователи со специальными правами доступа *JOBCTL могут блокировать, изменять, удалять и разблокировать буферные файлы в очереди вывода, но не могут просматривать, копировать, отправлять и перемещать эти буферные файлы. За счет этого операторам можно дать возможность управлять записями очереди вывода, не просматривая их содержимое.

Параметр очереди вывода Права на исправление (AUTCHK)

Параметр Права на исправление (AUTCHK) позволяет указать права доступа пользователя для изменения или удаления буферного файла в системе.

Параметр AUTCHK определяет, разрешено ли пользователю с правами доступа *READ, *ADD и *DLT по отношению к очереди вывода изменять и удалять буферные файлы других пользователей.

<i>Возможные значения параметра AUTCHK</i>	
*OWNER	Изменять и удалять буферные файлы других пользователей разрешено только владельцу очереди вывода.
*DTAAUT	Любой пользователь с правами доступа *READ, *ADD и *DLT по отношению к очереди вывода может изменять и удалять буферные файлы других пользователей.

Параметр очереди вывода Управляется оператором (OPRCTL)

Параметр Управляется оператором (OPRCTL) указывает, разрешено ли пользователю со специальными правами доступа *JOBCTL управлять очередью вывода.

<i>Возможные значения параметра OPRCTL</i>	
*YES	Пользователю со специальными правами *JOBCTL разрешено выполнять любые функции над буферными файлами, если параметр DSPDTA не равен *OWNER. Если параметр DSPDTA равен *OWNER, то прав доступа *JOBCTL недостаточно для просмотра, копирования, отправки и перемещения буферных файлов.
*NO	Специальные права доступа *JOBCTL не дают возможность выполнять операции над очередью вывода. Права доступа этого пользователя проверяются так же, как и у обычных пользователей.

Параметры очереди вывода и права доступа, необходимые для печати

В этом разделе описаны параметры очереди вывода и права доступа, необходимые для управления печатью.

В Табл. 124 на стр. 224 указано, какие параметры очереди вывода и права доступа к очереди вывода необходимы для выполнения функций управления печатью в системе. Для некоторых функций допустимо несколько сочетаний значений. Владелец буферного файла всегда разрешено выполнять все функции над файлом. Дополнительная информация приведена в разделе “Команды для работы с загрузчиками” на стр. 523.

В “Команды буферного файла” на стр. 508 указаны права доступа и параметры очереди вывода для всех команд работы с буферными файлами. Команды очереди вывода указаны в “Команды очереди вывода” на стр. 480.

Внимание: Для пользователя со специальными правами доступа *SPLCTL (права на управление буфером) не действуют никакие ограничения на доступ к очередям вывода. Специальные права доступа *SPLCTL позволяют выполнять любые операции над любыми очередями вывода. Права доступа *SPLCTL следует предоставлять только тем пользователям, которым они действительно необходимы.

Таблица 124. Права доступа, требуемые для функций печати

Функция печати	Параметры очереди вывода			Права доступа к очереди вывода	Специальные права доступа
	DSPDTA	AUTCHK	OPRCTL		
Добавление буферных файлов в очередь ¹				*READ	Нет
			*YES		*JOBCTL
Просмотр списка буферных файлов (команда WRKOUTQ ²)				*READ	Нет
			*YES		*JOBCTL
Просмотр, копирование и отправка буферных файлов (DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSPLF, ²)	*YES			*READ	Нет
	*NO	*DTAAUT		*READ, *ADD, *DLT	Нет
	*NO	*OWNER		Владелец ³	Нет
	*YES		*YES		*JOBCTL
	*NO		*YES		*JOBCTL
Изменение, удаление, блокирование и разблокирование буферного файла (CHGSPLFA, DLTSPLF, HLDSPFL, RLSSPLF ²)		*DTAAUT		*READ, *ADD, *DLT	Нет
		*OWNER		Владелец ³	Нет
			*YES		*JOBCTL
Изменение, очистка, блокирование и разблокирование очереди вывода (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ ²)		*DTAAUT		*READ, *ADD, *DLT	Нет
		*OWNER		Владелец ³	Нет
			*YES		*JOBCTL
Запуск загрузчика для очереди (STRPRTWTR, STRRMTWTR ²)		*DTAAUT		*CHANGE	Нет
			*YES		*JOBCTL
¹ Эти права доступа необходимы для размещения вывода в очереди вывода. ² Применение указанных команд или аналогичных опций меню. ³ Необходимо являться владельцем очереди вывода. ⁴ Дополнительно требуются права доступа *USE к описанию принтера. ⁵ Для *CHGOUTQ помимо прав доступа *READ, *ADD и *DLT необходимы права доступа *OBJMGT к очереди вывода.					

Примеры: очередь вывода

Ниже приведено несколько примеров настройки параметров защиты очередей вывода в различных ситуациях.

- Необходимо создать очередь вывода общего назначения. Всем пользователям разрешено просматривать буферные файлы. Системным операторам разрешено управлять очередью и изменять буферные файлы:

```
CRTOUTQ OUTQ(QGPL/GPOUTQ) DSPDTA(*YES) +
OPRCTL(*YES) AUTCHK(*OWNER) AUT(*USE)
```

- Необходимо создать очередь вывода приложения. Применять эту очередь вывода разрешено только элементам профайла группы GRPA. Всем пользователям, которым предоставлен доступ к очереди вывода, разрешено просматривать любые буферные файлы. Системным операторам запрещено работать с очередью вывода:

```
CRTOUTQ OUTQ(ARLIB/AROUTQ) DSPDTA(*YES) +
      OPRCTL(*NO) AUTCHK(*OWNER) AUT(*EXCLUDE)
GRTOBJAUT OBJ(ARLIB/AROUTQ) OBJTYP(*OUTQ) +
      USER(GRPA) AUT(*CHANGE)
```

- Необходимо создать очередь вывода для конфиденциальной информации, которую будет применять системный администратор для печати информации о пользовательских профайлах и правах доступа. Очередь вывода будет принадлежать профайлу QSECOFR, который ее создал.

```
CRTOUTQ OUTQ(QGPL/SECOUTQ) DSPDTA(*OWNER) +
      AUTCHK(*DTAAUT) OPRCTL(*NO) +
      AUT(*EXCLUDE)
```

Даже если системным администраторам предоставлены специальные права доступа *ALLOBJ, они не смогут работать с буферными файлами других пользователей из очереди вывода SECOUTQ.

- Необходимо создать очередь вывода, которая будет применяться несколькими пользователями для печати конфиденциальных файлов и документов. Пользователям должен быть предоставлен доступ только к собственным буферным файлам. Системным операторам разрешено работать с буферными файлами, но запрещено просматривать их содержимое.

```
CRTOUTQ OUTQ(QGPL/CFOUTQ) DSPDTA(*OWNER) +
      AUTCHK(*OWNER) OPRCTL(*YES) AUT(*USE)
```

Атрибуты сети

Сетевые атрибуты управляют обменом данными с другими системами.

Некоторые из них определяют способ обработки удаленных запросов на выполнение заданий и доступ к информации. Такие сетевые атрибуты напрямую влияют на защиту системы. Они описаны в следующих разделах:

- Действие над заданием (JOBACN)
- Обработка запросов клиентов (PCSACC)
- Обработка запросов DDM (DDMACC)

Ниже указаны возможные значения этих сетевых атрибутов. Значение по умолчанию подчеркнуто. Для изменения значения сетевого атрибута воспользуйтесь командой Изменить сетевой атрибут (CHGNETA).

Сетевой атрибут Действие над заданием (JOBACN)

Сетевой атрибут JOBACN определяет способ обработки поступающих запросов на запуск заданий.

Возможные значения для JOBACN:	
*REJECT	Входящие данные отклоняются. Отправителю и указанному получателю отправляется сообщение о том, что входящие данные были отклонены.
*FILE	Входящие данные сохраняются в очереди сетевых файлов того пользователя, которому они предназначены. Этот пользователь может просмотреть, отменить или принять входящие данные в файл базы данных, либо передать эти данные на обработку в очередь заданий. Отправителю и получателю отправляется сообщение о том, что входящие данные сохранены в файле.
*SEARCH	Выполняемые действия определяются значениями из таблицы сетевых заданий.

Рекомендации:

Если вы не планируете получать запросы на запуск удаленных заданий, то присвойте значение *REJECT сетевому атрибуту JOBACN.

Информация, связанная с данной



SNA Distribution Services

Сетевой атрибут Обработка запросов клиентов (PCSACC)

Сетевой атрибут PCSACC указывает, каким образом лицензионная программа System i Access для Windows обрабатывает запросы на доступ к объектам, поступающие от подключенных персональных компьютеров.

Этот атрибут определяет возможность доступа к объектам на платформе System i, а не возможность использования функции эмуляции рабочей станции.

Примечание: Сетевой атрибут PCSACC применяется только для клиентов DOS и OS/2. Этот атрибут никак не влияет на прочие клиенты System i Access.

Возможные значения для PCSACC:	
*REJECT	System i Access отклоняет все запросы персональных компьютеров на доступ к объектам на платформе System i. Приложению PC отправляется сообщение об ошибке.
*OBJAUT	Программа System i Access выполняет обычную процедуру проверки прав доступа для объекта, запрошенного программой PC. Например, если запрошена передача файла, то проверяется наличие прав на копирование данных из файла базы данных.
*REGFAC	Система запускает программу выхода, указанную в средстве регистрации системы. Если для точки выхода не определена никакая программа выхода, то вместо этого значения применяется значение *OBJAUT.
<i>полное- имя- программы</i>	Программа System i Access вызывает пользовательскую программу выхода, чтобы определить, следует ли отклонить запрос PC. Программа выхода вызывается только в том случае, если обычная процедура проверки прав доступа к объекту была успешно выполнена. Программа System i Access передает информацию о пользователе и запрошенной функции программе выхода. Программа выхода возвращает код, указывающий, следует ли принять или отклонить запрос. Если код возврата указывает на то, что запрос должен быть наклонен, либо если возникла ошибка, то на персональный компьютер отправляется сообщение об ошибке.

Возможные риски и рекомендации

В этом разделе приведены инструкции по защите файлов в системе.

Если в системе установлена программа System i Access, то обычных мер по защите системы может оказаться недостаточно. Так, если пользователю предоставлены права доступа *USE по отношению к файлу, а сетевой атрибут PCSACC равен *OBJAUT, то пользователь может передать весь файл на персональный компьютер, используя System i Access и программу на персональном компьютере. После этого пользователь может скопировать данные на дискету или магнитную ленту с помощью PC и вынести их за пределы офиса.

Пользователю System i с правами доступа *USE к файлу можно запретить копирование файла следующими способами:

- Указав параметр LMTCPB(*YES) в пользовательском профайле.
- Ограничив права доступа к командам копирования файлов.
- Ограничив права доступа к командам, применяемым программой System i Access.
- Аннулировав все предоставленные пользователю права доступа *ADD по отношению к каким-либо библиотекам. Права доступа *ADD необходимы для создания файла в библиотеке.

- Запретив пользователю доступ ко всем устройствам *SAVRST.

Ни один из перечисленных выше способов не действует в отношении пользователей PC, работающих с лицензионной программой System i Access. В этом случае единственный способ защиты заключается в создании программы выхода для проверки всех запросов.

Программа System i Access вызывает пользовательскую программу выхода, указанную в сетевом атрибуте PCSACC, при получении запросов на доступ к следующим функциям:

- Передача файлов
- Виртуальный принтер
- Сообщение
- Общая папка

Информация, связанная с данной

Программирование: iSeries Access

Сетевой атрибут Обработка запросов DDM (DDMACC)

Сетевой атрибут Обработка запросов DDM (DDMACC) определяет способ обработки запросов на доступ к данным через Управление распределенными данными (DDM) или функцию распределенной реляционной базы данных, поступающих от других систем.

<i>Возможные значения для DDMACC:</i>	
*REJECT	Система не принимает никакие запросы DDM и DRDA от удаленных систем. Значение *REJECT не препятствует выполнению функции инициатора и отправке запросов другим серверам.
*OBJAUT	Удаленные запросы обрабатываются в соответствии с правами доступа к объектам, настроенными в системе.
<i>полное- имя- программы</i>	После выполнения обычной процедуры проверки прав доступа к объекту вызывается указанная пользовательская программа выхода. Она применяется только для файлов DDM, но не для функций распределенной реляционной базы данных. Программе выхода передается список параметров, сформированный удаленной системой, в котором указан пользователь локальной системы и запрос. Программа выхода проверяет запрос и отправляет код возврата, разрешающий или запрещающий доступ к запрошенному объекту.

Информация, связанная с данной

Замечания о параметрах DDMACC

Операции сохранения и восстановления

Наличие возможности сохранять и восстанавливать объекты системы представляет потенциальную опасность для вашей организации.

Например, обычно программистам предоставлены права доступа *OBJEXIST по отношению к программам, так как эти права доступа необходимы для компиляции программы и удаления старой копии. Однако права доступа *OBJEXIST позволяют сохранить объект. Это значит, что такой программист может скопировать на магнитную ленту любые программы, в том числе и программы с очень высокой стоимостью.

Пользователю с правами доступа *OBJEXIST также разрешено восстанавливать объект с заменой существующего объекта. В нашем примере программист может восстановить программу, созданную в другой системе. Эта программа может выполнять совсем другие функции. Для примере предположим, что исходная программа применялась для работы с конфиденциальными данными. Новая версия программы может выполнять аналогичные функции и дополнительно копировать конфиденциальную информацию в

секретный файл, расположенный в библиотеке программиста. Программисту не требуются права доступа к конфиденциальным данным, так как к данным будут обращаться обычные пользователи программы.

Ограничение доступа к командам сохранения и восстановления

Для защиты системы можно ограничить доступ к командам сохранения и восстановления.

Доступ к операциям сохранения и восстановления объектов можно ограничить несколькими способами:

- Ограничьте физический доступ к устройствам сохранения и восстановления, таким как лентопротяжные устройства и оптические накопители.
- Ограничьте права доступа к описаниям устройств сохранения и восстановления. Для сохранения объекта на магнитной ленте необходимы права доступа *USE к описанию лентопротяжного устройства.
- Ограничьте доступ к командам сохранения и восстановления. Это позволит отслеживать, какие данные сохраняются и восстанавливаются в системе через любые интерфейсы, в том числе файлы сохранения. Соответствующий пример приведен в разделе “Пример: ограничение доступа к командам сохранения и восстановления”. При установке системы для команд восстановления задаются права доступа PUBLIC(*EXCLUDE).
- Предоставляйте специальные права доступа *SAVSYS только тем сотрудникам, которым вы доверяете.

Пример: ограничение доступа к командам сохранения и восстановления

В этом разделе приведен пример ограничения доступа к командам сохранения и восстановления.

Для того чтобы ограничить доступ к командам сохранения и восстановления в системе, выполните, например, следующие действия:

1. С помощью следующей команды создайте список прав доступа, с помощью которого вы будете предоставлять права доступа к командам системным операторам:
`CRTAUTL AUTL(SRLIST) TEXT('Список сохранения и восстановления')
AUT(*EXCLUDE)`
2. С помощью следующей команды настройте список прав доступа для защиты команд сохранения:
`GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) AUTL(SRLIST)`
3. Для того чтобы права доступа *PUBLIC определялись с помощью списка прав доступа, введите следующую команду:
`GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
AUT(*AUTL)`
4. Для настройки списка прав доступа для защиты команд восстановления введите следующую команду:
`GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) AUTL(SRLIST)`
5. Для того чтобы права доступа *PUBLIC определялись с помощью списка прав доступа, введите следующую команду:
`GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) USER(*PUBLIC)
AUT(*AUTL)`
6. Теперь для сохранения системы операторам должны быть предоставлены не только специальные права доступа *SAVSYS, но и права доступа к командам SAVxxx. Для предоставления прав доступа к этим командам нужно добавить системных операторов в список прав доступа:
`ADDAUTLE AUTL(SRLIST) USER(USERA USERB) AUT(*USE)`

Примечание: Системным операторам можно предоставить доступ только к командам сохранения. В этом случае для команд сохранения и команд восстановления нужно создать два отдельных списка прав доступа.

7. Для ограничения доступа к API сохранения и восстановления с помощью списка прав доступа введите следующие команды:

```

GRTOBJAUT OBJ(QSRSAV0) OBJTYPE(*PGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRSAV0) OBJTYPE(*PGM) USER(*PUBLIC)
  AUT(*AUTL)GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) USER(*PUBLIC)
  AUT(*AUTL)GRTOBJAUT OBJ(QSRRST0) OBJTYPE(*PGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRRST0) OBJTYPE(*PGM) USER(*PUBLIC)
  AUT(*AUTL)

```

Настройка производительности

Отслеживание и настройка производительности не входят в обязанности системного администратора. Однако системный администратор должен запретить пользователям изменять параметры производительности системы для ускорения выполнения собственных заданий за счет других заданий.

Производительность заданий в системе зависит от нескольких объектов управления заданиями:

- Класс задает приоритет запуска и квант времени для задания.
- Класс и пул памяти задания задаются в записи о выполнении, содержащейся в описании подсистемы.
- Описание задания может определять очередь вывода, приоритет вывода, очередь заданий и приоритет задания.

Знающие об этом пользователи с соответствующими правами доступа могут создать в системе собственную среду и обеспечить более высокую производительность для своих заданий, чем для заданий других пользователей. Для того чтобы это предотвратить, ограничьте права на создание и изменение объектов управления заданиями. Настройте общие права доступа *EXCLUDE для команд управления заданиями и предоставьте права доступа к этим командам узкому кругу доверенных пользователей.

Параметры производительности системы можно изменять в интерактивном режиме. Например, с помощью меню Работа с состоянием системы (WRKSYSSTS) можно изменить размер пулов памяти и уровни активности. Кроме того, пользователь со специальными правами доступа *JOBCTL (права на управление заданиями) может изменять приоритет планирования любого задания в системе при условии соблюдения ограничения на приоритет (PTYLMT), заданного в пользовательском профайле. Будьте внимательны при предоставлении прав доступа *JOBCTL и настройке параметра PTYLMT в пользовательских профайлах.

Для того чтобы разрешить пользователям просматривать информацию о производительности с помощью команды WRKSYSSTS и запретить изменять эту информацию, введите следующую команду:

```

GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
  USER(*PUBLIC) AUT(*EXCLUDE)

```

Разрешите пользователям, отвечающим за настройку производительности системы, изменять параметры производительности:

```

GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
  USER(USRTUNE) AUT(*USE)

```

Выполнение заданий только в пакетном режиме

Вы можете создать или изменить команды, чтобы разрешить некоторым заданиям выполняться только в пакетной среде.

Например, в пакетном режиме может выполняться создание отчетов или компиляция программ. При выполнении в пакетном режиме задание обычно меньше влияет на производительность системы, чем при выполнении в интерактивном режиме.

Например, для того чтобы команда, запускающая программу RPTA, выполнялась только в пакетном режиме, выполните следующие действия:

- Создайте команду запуска RPTA и укажите, что эта команда может выполняться только в пакетном режиме:

```
CRTCMD CMD(RPTA) PGM(RPTA) ALLOW(*BATCH *BPGM)
```

Для того чтобы все операции компиляции выполнялись в пакетном режиме, введите следующую команду для каждого типа программ:

```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
```

Глава 7. Разработка схем защиты

В этом разделе приведены рекомендации, которые помогут разработчикам приложений и системным администраторам включить необходимые средства защиты в состав приложений. Раздел также содержит примеры решения некоторых задач по защите системы.

Защита информации - это важная составная часть многих приложений. Требования к защите, наряду с другими требованиями, необходимо учитывать на этапе разработки приложений. Например, при выборе способа хранения данных приложения в библиотеках следует принять во внимание как требования к защите, так и другие требования к приложению - например, к его производительности, а также к резервному копированию и восстановлению.

В некоторых примерах этого раздела приведены программы. Они приведены только для наглядности изложения. Для успешной компиляции и запуска большинства из этих программ в них необходимо внести некоторые изменения; кроме того, программы не содержат функции обработки сообщений и исправления ошибок.

Раздел Планирование и настройка защиты системы справочной системы Information Center предназначен для администратора защиты. Он содержит формы, примеры и рекомендации по планированию защиты уже существующих приложений. Приведенные в разделе Планирование и настройка защиты системы формы и примеры могут быть интересны и проектировщикам приложений. Они помогут взглянуть на приложение с точки зрения администратора защиты и понять, какую информацию вам необходимо предоставить.

Раздел Планирование и настройка защиты системы справочной системы Information Center также содержит набор примеров программ для вымышленной компании JKL Toys. В этом разделе для иллюстрации используется аналогичный набор примеров программ. В рис. 31 описана взаимосвязь между группами пользователей, приложениями и библиотеками компании JKL Toys описана:

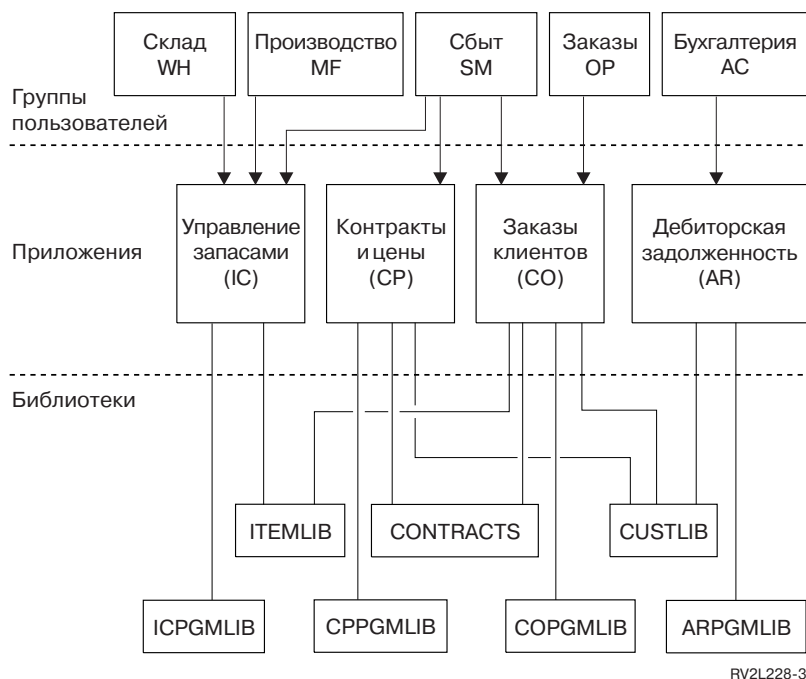


Рисунок 31. Примеры приложений

Описание графика

На этом графике приведена схема доступа пяти групп пользователей к приложениям и библиотекам в системе компании JKL Toys. Все пользователи делятся на пять групп - Склад, Производство, Отдел сбыта, Заказы и Бухгалтерия. Эти группы пользователей имеют различные права доступа к разным приложениям, как показано далее.

- У пользователей из групп Склад, Производство и Отдел сбыта есть права доступа к приложениям Управления запасами.
- Пользователи из группы Отдел сбыта также могут работать с приложениями Контракты и цены и Заказы клиентов.
- С последним приложением также могут работать пользователи из группы Заказы.
- У пользователей из группы Бухгалтерия есть права доступа только для работы с приложением Дебиторская задолженность.

Информация, связанная с данной

Сценарии для HTTP Server

Общие рекомендации по проектированию защиты

Отсутствие сложных решений в реализации защиты системы позволяет значительно упростить управление средствами защиты и контроль за их применением. Кроме того, это существенно повышает производительность приложений и операций резервного копирования.

Ниже приведены общие рекомендации по организации защиты:

- Для защиты информации можно применять средства защиты ресурсов, а также доступные методы защиты, такие как ограничение возможностей пользовательского профайла и предоставление пользователям доступа лишь к некоторым меню системы.

Attention: Если в системе применяется продукт System i Access или к системе подключены линии связи, то ограничение возможностей пользовательского профайла и запрет доступа к некоторым меню системы не позволяет обеспечить необходимый уровень защиты системы. Для того чтобы предотвратить доступ к объектам системы с помощью этих интерфейсов, необходимо воспользоваться средствами защиты ресурсов.

- Следует включать средства защиты только для тех объектов, защита которых действительно необходима. Проанализируйте библиотеку и определите, какие объекты (например, файлы данных) являются конфиденциальными, и примените средства защиты только к этим объектам. Для остальных объектов, таких как области данных и очереди сообщений, задайте общие права доступа.
- Переходите от общего к частному:
 - Спланируйте защиту библиотек и каталогов. Настраивайте параметры защиты отдельных объектов только в особых случаях.
 - Вначале спланируйте общие права доступа, затем - права доступа групп, а затем - права доступа отдельных пользователей.
- Установите для новых объектов библиотеки такие же общие права доступа (параметр CRTAUT), как общие права доступа к большинству существующих объектов библиотеки.
- Для упрощения контроля и повышения производительности операций проверки прав доступа не определяйте частные права доступа к объекту, уровень которых ниже, чем общие права доступа.
- Объедините объекты с одинаковыми требованиями к защите в группы с помощью списков прав доступа. Такими списками проще управлять, чем правами доступа к отдельным объектам, и они позволяют восстанавливать параметры защиты.

Понятия, связанные с данным

Глава 5, “Защита ресурсов”, на стр. 137

В этом разделе описаны все компоненты защиты ресурсов и приведена информация об их совместном применении для защиты информации в системе. Кроме того, здесь вы сможете найти сведения о настройке защиты ресурсов с помощью команд и меню CL.

Планирование изменения уровня пароля

Изменение уровня паролей необходимо тщательно запланировать. Необдуманное изменение уровня пароля может привести к сбоям при взаимодействии с другими системами или к ошибкам при входе пользователей в систему.

Перед изменением системного значения QPWLVL сохраните данные о защите системы с помощью команды SAVSECDTA или SAVSYS. Наличие резервной копии данных позволяет сбросить пароли всех пользовательских профайлов и восстановить более низкий уровень паролей.

В работе продуктов системы и ее клиентов могут возникать ошибки, если системное значение Уровень паролей (QPWLVL) равно 2 или 3. Все продукты и клиенты, отправляющие пароли системе в зашифрованном виде, необходимо обновить в соответствии с правилами шифрования паролей уровня 2 или 3. Отправка зашифрованных паролей называется подстановкой паролей. Подстановка паролей применяется для защиты паролей при их передаче по сети. Пароль, зашифрованный клиентской программой старой версии, не поддерживающей алгоритм шифрования, не будет принят сервером, даже если он содержит только допустимые символы. Это относится и к обмену данными между двумя равноправными узлами System i, в ходе которого для идентификации систем System i применяются зашифрованные значения.

Несовместимость паролей разных уровней влияет и на работу тех продуктов, которые служат для создания других программ (например, IBM Toolbox for Java). Продукты других фирм, использующие такое программное обеспечение предыдущих версий, будут работать правильно только после его обновления.

Если принять во внимание эти и некоторые другие факторы, становится очевидно, что изменять системное значение QPWLVL следует с особой осторожностью.

Изменение значения QPWLVL с 0 на 1

Если в системе применяются пароли уровня 1 и система не обменивается данными с продуктом System i Support for Windows Network Neighborhood (NetServer), то пароли NetServer можно удалить. Удаление ненужных зашифрованных паролей из системы позволяют повысить общий уровень ее защиты.

Если системное значение QPWLVL равно 1, то в системе можно использовать все текущие (предназначенные для выпусков до V5R1) алгоритмы идентификации и шифрования паролей. Ошибки могут возникать лишь в работе тех функций и служб, для которых требуется пароль NetServer.

Изменение значения QPWLVL с 0 или 1 на 2

Уровень паролей 2 позволяет применять пароли с учетом регистра длиной до 128 символов (их также называют паролями-предложениями) и предоставляет наиболее широкие возможности для возврата к значению QPWLVL 0 или 1.

Независимо от уровня паролей системы, пароли уровней 2 и 3 создаются при изменении пароля и при входе пользователя в систему. Создание паролей уровней 2 и 3 в системе с уровнем паролей 0 или 1 позволяет подготовить систему к переходу на уровень паролей 2 или 3.

Перед тем как изменить значение QPWLVL на 2, администратор системы должен найти все пользовательские профайлы, не содержащие пароль, который можно применять на уровне паролей 2. Это можно сделать с помощью команды PRTUSRPRF TYPE(*PWDLVL). В зависимости от типов найденных профайлов администратор может добавить в них пароль уровня 2 или 3 одним из следующих способов.

- Изменить пароль пользовательского профайла с помощью команды CL CHGUSRPRF или CHGPWD, либо API QSYCHGPW. При этом будет изменен пароль уровня 0 или 1; кроме того, будут созданы два эквивалентных пароля уровней 2 и 3 с учетом регистра символов. Для уровней 2 и 3 будут созданы версии пароля, содержащие только прописные и только строчные символы.

Например, если новое значение пароля - C4D2RB4Y, в системе будут созданы пароли уровня 2 C4D2RB4Y и c4d2rb4y.

- Войти в систему с помощью алгоритма, при котором пароль не шифруется (не применяется подстановка паролей). Если пароль указан верно, и в пользовательском профайле нет пароля, который можно применять на уровне 2 или 3, то в системе будут созданы два эквивалентных пароля, в которых будет учитываться регистр символов; эти пароли можно будет применять на уровне 2 и 3. Будут созданы версии паролей со всеми строчными и всеми прописными символами.

Если в профайле нет пароля уровня 0 или 1 или если пользователь попытается войти в систему с помощью продукта, применяющего подстановку паролей, то отсутствие в профайле пароля уровня 2 или 3 может стать причиной неполадки. В этих случаях пользователь не сможет войти в систему, если будет установлен уровень паролей 2.

Если пользовательский профайл отвечает следующему описанию, то будет выполнена проверка пароля в соответствии с правилами для паролей уровня 0, а в пользовательском профайле будет создано два пароля уровня 2, как описано выше.

- Для пользовательского профайла не задан пароль уровня 2 или 3.
- Для пользовательского профайла задан пароль уровня 0 или 1.
- Пользователь входит в систему с паролем, передаваемым открытым текстом.

После этого при входе пользователя в систему будет выполняться проверка пароля уровня 2.

Если какие-либо клиенты не были обновлены для применения нового алгоритма подстановки паролей (паролей-предложений), то на уровне паролей QPWDLVL 2 такие клиенты будут работать неправильно. Администратор должен убедиться в том, что клиенты были обновлены для применения нужного алгоритма подстановки паролей.

К числу клиентов, использующих подстановку паролей, относятся:

- TELNET
- System i Access
- System i Host Servers
- QFileSrv.400
- Функция печати System i NetServer
- DDM
- DRDA
- SNA LU6.2

Перед установкой в системе уровня паролей 2 настоятельно рекомендуется сохранить все данные о защите. Это позволит существенно упростить обратный переход к уровню QPWDLVL 0 или 1, если когда-либо возникнет необходимость в таком переходе.

| Изменяйте системные значения паролей, такие как QPWDMINLEN, QPWDMAXLEN и QPWDRULES, только
| после проверки QPWDLVL 2. Это позволит упростить возврат к значению QPWDLVL 1 или 0, если
| возникнет необходимость в таком возврате. Тем не менее, для того, чтобы можно было присвоить
| QPWDLVL значение 2, системное значение QPWDVLDPGM должно быть равно *REGFAC или *NONE.
| Следовательно, если в системе применяется программа проверки паролей, то можно создать новую
| программу, а затем зарегистрировать ее для точки выхода QIBM_QSY_VLD_PASSWRD с помощью
| команды ADDEXITPGM.

На уровне QPWDLVL 2 поддерживаются пароли NetServer, поэтому все функции и службы, которым необходим пароль NetServer, будут работать правильно.

Если работа системы на уровне QPWDLVL 2 не вызывает нареканий, то можно приступить к изменению остальных системных значений с целью поддержки длинных паролей. Однако учтите, что при переходе к длинным паролям может произойти следующее:

- При применении паролей длиннее 10 символов пароли уровня 0 или 1 удаляются. Пользователи профайлов с такими паролями не смогут войти в систему после восстановления уровня паролей 0 или 1.
- Если пароли содержат специальные символы или не соответствуют правилам создания простых имен объектов (за исключением правила учета регистра), пароли уровня 0 и 1 удаляются.
- При указании пароля длиннее 14 символов пароль NetServer для пользовательского профайла удаляется.
- Системные значения паролей применяются только к новым паролям уровня 2 и не применяются к созданным системой паролям уровня 0 и 1 и паролям NetServer (если такие пароли созданы).

Изменение значения QPWDLVL с 2 на 3

Если на уровне QPWDLVL 2 система работает достаточно стабильно, можно перейти на уровень QPWDLVL 3 для повышения надежности защиты паролей.

На уровне QPWDLVL 3 все пароли NetServer удаляются, поэтому переводить систему в режим QPWDLVL 3 следует только в случае, если пароли NetServer не применяются.

На уровне QPWDLVL 3 все пароли уровней 0 и 1 удаляются. С помощью команд DSPAUTUSR или PRTUSRPRF администратор может найти профайлы, в которых нет паролей уровня 2 или 3.

Переход с уровня QPWDLVL на более низкий уровень пароля

Даже в тех случаях, когда возврат к более низкому уровню паролей возможен, он сопряжен с определенными трудностями. Следует помнить, что, как правило, при увеличении значения QPWDLVL обратная операция невозможна. Тем не менее, в некоторых случаях можно уменьшить значение QPWDLVL.

Изменение значения QPWDLVL с 3 на 2

Выполнить такой переход относительно несложно. Если значение QPWDLVL равно 2, то администратор должен определить, требуется ли какому-либо пользовательскому профайлу пароль NetServer или пароль уровня 1 или 0, и если да, то изменить пароль в профайле на допустимое значение.

Кроме того, если в системе будут применяться пароли NetServer или пароли уровня 0 или 1, то может потребоваться восстановить совместимые с ними системные значения паролей.

Изменение значения QPWDLVL с 3 на 1 или 0

Поскольку переход с уровня паролей 3 на уровень 0 или 1 может привести к серьезным неполадкам в работе системы (например, ни один пользователь не сможет войти в систему, так как все пароли уровня 0 и 1 ранее были удалены), прямой переход не поддерживается. Для перехода с уровня QPWDLVL 3 на уровень QPWDLVL 1 или 0 необходимо сначала перейти на промежуточный уровень QPWDLVL 2.

Изменение значения QPWDLVL с 2 на 1

Перед тем как изменить QPWDLVL на 1, необходимо найти все профайлы, в которых нет паролей уровня 0 или 1, с помощью команд DSPAUTUSR или PRTUSRPRF TYPE(*PWDINFO). Если после изменения системного значения QPWDLVL пользовательский профайл должен будет содержать пароль, необходимо создать в профайле пароль уровня 0 или 1 одним из следующих способов:

- Изменить пароль пользовательского профайла с помощью команды CL CHGUSRPRF или CHGPWD, либо API QSYCHGPW. При этом в системе будет изменен пароль уровня 2 и 3; кроме того, в системе будет создан эквивалентный пароль в верхнем регистре, который можно применять на уровнях 0 и 1. Пароль для уровней 0 и 1 создается только в том случае, если выполнены следующие условия:
 - Длина пароля не превосходит 10 символов.
 - Все символы пароля можно преобразовать в символы EBCDIC A-Z, 0-9, @, #, \$ или символ подчеркивания.
 - В качестве первого символа пароля не указана цифра или символ подчеркивания.

Например, если новое значение пароля - RainyDay, то для уровней 0 и 1 в системе будет создан пароль RAINYDAY. Однако при изменении пароля на Rainy Days In April система удалит пароль уровней 0 и 1 (поскольку длина пароля слишком велика и он содержит пробелы).

Если системе не удалось создать пароль уровня 0 или 1, она не отправляет об этом никаких сообщений.

- Войти в систему с помощью алгоритма, при котором пароль не шифруется (не применяется подстановка паролей). Если пароль указан верно, и в профайле нет пароля уровня 0 или 1, то системой будет создан эквивалентный пароль для уровней 0 и 1 в верхнем регистре. Пароль для уровней 0 и 1 создается только в том случае, если выполнены все указанные выше условия.

После этого системное значение QPWLVL можно изменить на 1. Когда новое значение вступит в силу (при следующей IPL), все пароли NetServer будут удалены.

Изменение значения QPWLVL с 2 на 0

Эта операция аналогична изменению значения QPWLVL с 2 на 1, за исключением того, что все пароли NetServer сохраняются после вступления изменений в силу.

Изменение значения QPWLVL с 1 на 0

После изменения значения QPWLVL на 0 необходимо найти в системе те пользовательские профайлы, в которых не задан пароль NetServer. Это можно сделать с помощью команды DSPAUTUSR или PRTUSRPRF. Если пользовательскому профайлу необходим пароль NetServer, то этот пароль можно создать, изменив пароль пользователя или войдя в систему с помощью инструмента, в котором не применяется шифрование паролей.

После этого можно присвоить QPWLVL значение 0.

Планирование библиотек

Структура библиотеки аналогична структуре каталога, позволяющего искать размещенные в нем объекты. Способ объединения информации приложения в библиотеки и управления библиотеками зависит от большого числа факторов.

Защита библиотек является эффективной только в том случае, если выполнены следующие условия:

- Библиотеки содержат объекты со схожими требованиями к защите.
- Пользователям запрещено добавлять новые объекты в библиотеки, доступ к которым ограничен. Все изменения программ в библиотеках отслеживаются. Это означает, что для библиотек приложений необходимо задать общие права доступа *USE или *EXCLUDE, за исключением тех случаев, когда пользователям нужно создавать объекты непосредственно в библиотеке.
- Отслеживаются списки библиотек.

Для обращения к объекту необходимы права доступа к самому объекту и к содержащей его библиотеке. Доступ к объекту можно запретить, ограничив права доступа к объекту и/или его библиотеке.

При наличии прав доступа *USE к библиотеке пользователь может выполнять поиск объектов в этой библиотеке. Права доступа к объекту определяют, *какие операции* можно выполнять над этим объектом. Прав доступа *USE к библиотеке достаточно для выполнения большинства операций с объектами в этой библиотеке.

Во многих случаях простым и эффективным способом защиты данных является предоставление общих прав доступа к объектам и ограничение доступа к библиотекам. Размещение программ отдельно от других объектов приложения также позволяет упростить планирование защиты. Это особенно эффективно работает в том случае, когда некоторые файлы применяются несколькими приложениями. С помощью прав доступа к библиотекам, содержащим прикладные программы, можно управлять доступом пользователей к приложениям.

Ниже приведены два примера защиты библиотек приложений компании JKL Toys. (Диаграмма приложений приведена в разделе рис. 31 на стр. 231.)

- Библиотека CONTRACTS содержит конфиденциальную информацию. Для работы с приложением Контракты и цены пользователям достаточно общих прав доступа к объектам библиотеки (*CHANGE). При этом для библиотеки CONTRACTS установлены общие права доступа *EXCLUDE. Права доступа *USE к библиотеке предоставляются только тем пользователям и группам, которым разрешено работать с приложением Контракты и цены.
- Компания JKL Toys - это небольшая компания, в которой доступ к информационным ресурсам, за исключением сведений о контрактах и ценах, предоставляется без существенных ограничений. Все пользователи системы могут просматривать данные о заказчиках и складе; изменять эти сведения могут только пользователи с соответствующими правами доступа. Для библиотек CUSTLIB и ITEMLIB, а также для всех объектов в этих библиотеках, заданы общие права доступа *USE. Пользователи могут просматривать сведения в этих библиотеках с помощью основных приложений и с помощью запросов SQL. Для библиотек программ заданы общие права доступа *EXCLUDE. К библиотеке ICPGMLIB могут обращаться только те пользователи, которым разрешено изменять информацию о содержимом склада. Программы, с помощью которых изменяется эта информация, принимают права доступа владельца приложения (OWNIC), поэтому у этих программ есть права доступа *ALL к файлам в библиотеке ITEMLIB.

Понятия, связанные с данным

“Защита библиотек” на стр. 141

Защита библиотек обеспечивает конфиденциальность информации.

Ссылки, связанные с данной

“Списки библиотек” на стр. 218

Список библиотек задания определяет набор библиотек, просматриваемых при поиске, и порядок просмотра библиотек.

Информация, связанная с данной

Сценарии для HTTP Server

Планирование приложений, позволяющее избежать создания профайлов больших размеров

Для того чтобы избежать снижения производительности и ухудшения защиты системы, при планировании приложений следует избегать создания профайлов больших размеров.

Поскольку это может повлиять на производительность и защиту системы, рекомендуется следовать следующим правилам, чтобы избежать чрезмерного роста размера профайлов:

- Не создавайте один профайл владельца для всех приложений.
Создайте отдельные пользовательские профайлы для своих приложений. Наличие разных профайлов владельцев у приложений упрощает восстановление этих приложений и их перенос между системами. При этом данные о частных правах доступа распределяются между несколькими профайлами, что также повышает производительность. Применение нескольких профайлов владельцев позволяет предотвратить создание слишком большого профайла, содержащего большое количество объектов. Кроме того, создание разных профайлов владельцев позволяет не предоставлять приложению излишне широкий набор принятых прав доступа.
- Не следует назначать владельцами приложений поставляемые фирмой IBM пользовательские профайлы, такие как QSECOFR и QPGMR.
Поскольку этим профайлам принадлежит большое количество поставляемых фирмой IBM объектов, это может значительно усложнить управление этими профайлами. Кроме того, это может привести к возникновению неполадок защиты при переносе приложений в другую систему. Назначение владельцами приложений поставляемые IBM пользовательские профайлы также может повлиять на скорость выполнения таких команд, как CHKOBJTG и WRKOBJOWN.
- Для защиты объектов следует применять списки прав доступа.

Если нескольким пользователям необходимо предоставить частные права доступа ко многим объектам, то для защиты этих объектов рекомендуется создать список прав доступа. При этом в пользовательском профайле будет создаваться одна запись о частных правах доступа для списка, а не множество записей для всех объектов. Кроме того, если применяются списки прав доступа, то в профайле владельца объекта создаются записи обо всех пользователях, которым предоставлен доступ к списку прав доступа.

Списки библиотек

Применение списков библиотек заданий обеспечивает дополнительную гибкость при работе с системой, но также может ослабить защиту. Это особенно важно помнить в тех случаях, когда для объектов установлены общие права доступа, а защита информации в основном полагается на защиту библиотек. В этом случае пользователи с правами доступа к библиотеке обладают неограниченным доступом к данным в этой библиотеке.

Для предотвращения опасностей, связанных с применением списков библиотек, в приложениях можно указывать полные имена. Если указано как имя объекта, так и имя библиотеки, то система не выполняет поиск объекта в списке библиотек. Это позволяет предотвратить обход защиты с помощью списка библиотек.

Тем не менее, другие требования к разработке приложений могут привести к отказу от применения полных имен. Если в приложениях применяются списки библиотек, то ознакомьтесь с приведенными в следующих разделах способами повышения уровня защиты системы.

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе Глава 10, “Лицензия на исходный код и отказ от обязательств”, на стр. 325.

Управление списком пользовательских библиотек

В качестве дополнительной меры защиты перед запуском задания можно обеспечить такой пользовательский список библиотек, который содержит нужные записи в правильном порядке. Для этого можно сохранить пользовательский список библиотек с помощью команды CL, заменить его на нужный список и восстановить прежний список после завершения работы приложения.

Ниже приведен пример программы, выполняющей перечисленные действия:

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе Глава 10, “Лицензия на исходный код и отказ от обязательств”, на стр. 325.

```

PGM
DCL      &USRLIBL *CHAR LEN(2750)
DCL      &CURLIB  *CHAR LEN(10)
DCL      &ERROR  *LGL
DCL      &CMD    *CHAR LEN(2800)
MONMSG   MSGID(CPF0000) +
        EXEC(GOTO SETERROR)
RTVJOBA  USRLIBL(&USRLIBL) +
        CURLIB(&CURLIB)
IF COND(&CURLIB=('*NONE')) +
    THEN(CHGVAR &CURLIB '*CRTDFT ')
CHGLIBL  LIBL(QGPL) CURLIB(*CRTDFT)
/*****/
/*      */
/*  Выполнение необходимых действий*/
/*      */
/*****/
GOTO     ENDPGM
SETERROR: CHGVAR  &ERROR '1'
ENDPGM:  CHGVAR  &CMD +
        ('CHGLIBL LIBL+
        (' *CAT &USRLIBL *CAT') +
        CURLIB(' *CAT &CURLIB *TCAT ' )')
CALL     QCMDEXC PARM(&CMD 2800)
IF       &ERROR SNDPGMMSG MSGID(CPF9898) +
        MSGF(QCPFMSG) MSGTYPE(*ESCAPE) +
        MSGDTA('The xxxx error occurred')
ENDPGM

```

Рисунок 32. Программа для замены и восстановления списка библиотек

Notes:

1. Независимо от способа завершения работы программы (обычного или аварийного), будет восстановлена та версия списка библиотек, которая применялась в момент запуска программы. Причина этого состоит в том, что процедура обработки ошибок включает операцию восстановления списка библиотек.
2. Поскольку в команде CHGLIBL необходимо указать список имен библиотек, ее нельзя запускать напрямую. Для получения списка библиотек, передаваемых команде CHGLIBL в качестве переменной, применяется команда RTVJOBA. Переменная передается функции QCMDEXC в качестве параметра.
3. Если в середине программы вызывается неконтролируемая функция выхода (например, пользовательская программа, меню, позволяющее запускать команды, или меню ввода команд), то для обеспечения надежной защиты программа должна заменять список библиотек после завершения работы этой функции.

Изменение списка системных библиотек

В этом разделе описана процедура изменения системной части списка библиотек, требуемого для защиты системы.

Если приложению необходимо добавить записи в системную часть списка библиотек, вы можете воспользоваться программой CL, аналогичной приведенной в разделе рис. 32, со следующими изменениями:

- Замените команду RTVJOBA на команду Получить системные значения (RTVSYVAL) для получения системного значения QSYSLIBL.
- Установите нужное значение системной части списка библиотек с помощью команды Изменить список системных библиотек (CHGSYSLIBL).
- В конце программы еще раз воспользуйтесь командой CHGSYSLIBL для восстановления исходного значения системной части списка библиотек.
- Команда CHGSYSLIBL поставляется с общими правами доступа *EXCLUDE. Для применения этой команды в программе выполните следующие действия:

- Предоставьте владельцу программы права доступа *USE к команде CHGSYSLIBL и воспользуйтесь принятыми правами доступа.
- Предоставьте пользователям, использующим программу, права доступа *USE к команде CHGSYSLIBL.

Сведения для защиты библиотек

Одной из задач разработчиков приложений является предоставление сведений о библиотеках администраторам защиты. С помощью этих сведений администратор защиты разрабатывает схему защиты библиотеки и ее объектов.

Как правило, в составе этих сведений необходимо указать:

- Функции приложений, добавляющие объекты в библиотеку.
- Данные о том, удаляются ли при обработке приложений содержащиеся в библиотеке объекты.
- Профайл, которому принадлежит библиотека и ее объекты.
- Сведения о том, следует ли включить библиотеку в списки библиотек.

На рис. 33 приведен пример формата, в котором может быть предоставлена такая информация:

```
Имя библиотеки: ITEMLIB
Общие права доступа к библиотеке: *EXCLUDE
Общие права доступа к объектам библиотеки: *CHANGE
Общие права доступа к новым объектам (CRTAUT): *CHANGE
Владелец библиотеки: OWNIC
```

Включить в списки библиотек? Нет. Библиотека добавляется в список библиотек начальной прикладной программой или начально программой запросов.

Функции, для применения которых необходимы права доступа *ADD к библиотеке:

Во время выполнения приложения объекты в библиотеку не добавляются. Объекты, для работы с которыми необходимы права доступа *OBJMGT и *OBJEXIST, и функции, которым необходимы эти права доступа:

Все рабочие файлы, имена которых начинаются с символов ICWRK, удаляются в конце месяца. Для этого необходимы права доступа *OBJMGT.

Рисунок 33. Формат сведений для защиты библиотеки

Планирование меню

Меню являются хорошим способом предоставления управляемого доступа к системе. Они позволяют предоставить пользователю доступ к фиксированному набору строго контролируемых функций, ограничив возможности пользователя и задав начальное меню в пользовательском профайле.

Для того чтобы меню можно было использовать в качестве средства управления доступом, при их разработке необходимо следовать приведенным ниже рекомендациям:

- Не включайте в состав меню, предназначенных для пользователей с ограниченными возможностями, интерфейс командной строки.
- Не включайте в одно меню функции с разными требованиями к защите. Например, если некоторым пользователям приложений разрешено только просматривать информацию, не изменяя ее, то для этих пользователей необходимо создать отдельное меню, позволяющее только просматривать и печатать сведения.
- Убедитесь, что все связанные меню содержат необходимые перекрестные ссылки, позволяющие пользователю открыть любое меню без применения командной строки.

- Предоставляйте доступ только к некоторым системным функциям, таким как просмотр вывода на принтер. Эта функция предусмотрена в меню ASSIST, которое можно указать в пользовательском профайле в качестве программы обработки нажатия клавиши Attention. Если пользовательский профайл относится к классу *USER и обладает ограниченными возможностями, то пользователь не может просматривать вывод и задания других пользователей.
- Включите в состав меню средства для работы с инструментами для принятия решений. Соответствующий пример приведен в разделе “Применение принятых прав доступа при разработке меню” на стр. 242.
- Возможно, следует предоставить пользователям доступ к меню Системный запрос или некоторым его функциям.
- Для пользователей, которым разрешено применять только одну функцию, не следует создавать меню; достаточно указать в пользовательском профайле начальную программу. В качестве начального меню укажите значение *SIGNOFF.

Например, все пользователи в компании JKL Toys могут работать с меню вопросов, предоставляющим доступ к большинству файлов. Для пользователей, которым не разрешено изменять данные, это меню является начальным. При выборе опции возврата в данном меню пользователь выходит из системы. Остальные пользователи могут открыть это меню, выбрав опцию вопроса в меню приложения. При нажатии клавиши F12 (Возврат) пользователь возвращается в предыдущее меню. Поскольку к библиотекам программ применяются правила защиты библиотек, это меню и вызываемые с его помощью программы хранятся в библиотеке QGPL:



Рисунок 34. Пример меню вопросов

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе Глава 10, “Лицензия на исходный код и отказ от обязательств”, на стр. 325.

Ссылки, связанные с данной

“Ограничить возможности” на стр. 87

С помощью поля Ограничить возможности вы можете ограничить доступ пользователя к командной строке на ввод команд и переопределение начальной программы, начального меню, текущей библиотеки и программы обработки клавиши Attention, указанной в пользовательской профайле. Это поле представляет собой инструмент, позволяющий ограничить возможности пользователя по изменению параметров системы.

Информация, связанная с данной

Сценарии для HTTP Server

Сведения для защиты меню

Одной из задач разработчиков приложений является предоставление сведений о меню администраторам защиты. С помощью этих сведений администратор защиты составляет список пользователей, которым разрешено работать с меню, и определяет необходимые для этого права доступа.

Ниже перечислены возможные типы сведений, требуемые администратору защиты:

- Необходимы ли для доступа к каким-либо функциям меню специальные права доступа, такие как *SAVSYS или *JOBCTL.

- Можно ли с помощью меню запустить программы, использующие принятые права доступа.
- Какие права доступа к объектам необходимы для применения каждой опции меню. Необходимо указать только права доступа, превышающие стандартные общие права доступа.

На рис. 35 приведен пример формата, в котором может быть предоставлена такая информация:

```
Имя меню: MENU1           Библиотека:  QGPLНомер опции:  3           Описание:  Запрос
Вызываемая программа: QRYSTART   Библиотека:  QGPL
Принятые права доступа: QRYUSR
Необходимые специальные права доступа:  Нет
Необходимые права доступа к объекту:  Пользователю необходимы права
доступа *USE к программе QRYSTART.
У пользователя QRYUSR должны быть права
доступа *USE к библиотекам, содержащим
запрашиваемые файлы. У
пользователя, профайла QRYUSR или всех пользователей должны быть права
доступа *USE к
запрашиваемым файлам.
```

Рисунок 35. Формат для требований меню защиты

Применение принятых прав доступа при разработке меню

Предоставление доступа к средствам поддержки принятия решений, таким как Query/400, предъявляет дополнительные требования к организации защиты. Средства защиты ресурсов не позволяют предоставлять пользователю разные права доступа к файлу в различных ситуациях. Тем не менее, используя принятые права доступа можно настроить такие права доступа, которые необходимы в конкретной ситуации.

Например, пользователям можно предоставить возможность просмотра файлов с помощью утилиты запросов, но при этом необходимо, чтобы эти файлы можно было изменять только с помощью протестированных прикладных программ.

Примечание: В разделе “Объекты, принимающие права доступа владельца” на стр. 156 приведено описание принятых прав доступа. В разделе “Блок-схема 8: Проверка принятых прав доступа” на стр. 191 описан алгоритм проверки принятых прав доступа.

На рис. 36 приведен пример начального меню, которое предоставляет управляемый доступ к файлам посредством утилит запросов, используя принятые права доступа:

```
MENU1           Начальное меню

1.  Управление запасами (ICSTART)
2.  Заказы клиентов      (COSTART)
3.  Запрос                (QRYSTART)
4.  Офис                  (OFCSTART)

(командная строка отсутствует)
```

Рисунок 36. Пример начального меню

Программы, с помощью которых запускаются приложения (ICSTART и COSTART), принимают права доступа профайла, которому принадлежат объекты приложений. Эти программы добавляют библиотеки приложений в список библиотек и показывают начальное меню приложения. Ниже приведен пример программы управления запасами (ICSTART).

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе Глава 10, “Лицензия на исходный код и отказ от обязательств”, на стр. 325.

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE ICPGMLIB
GO ICMENU
RMVLIBLE ITEMLIB
RMVLIBLE ICPGMLIB
ENDPGM
```

Рисунок 37. Пример прикладной программы

Программа, запускающая запрос (QRYSTART), принимает права доступа профайла (QRYUSR), который служит для доступа к файлам при обработке запросов. На рисунке рис. 38 показана программа QRYSTART:

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE CUSTLIB
STRQRY
RMVLIBLE ITEMLIB
RMVLIBLE CUSTLIB
ENDPGM
```

Рисунок 38. Пример программы для запроса, применяющей принятые права доступа

Система меню поддерживает работу с тремя типами пользовательских профайлов, описанными в Табл. 125. В Табл. 126 описаны объекты, применяемые в системе меню.

Таблица 125. Пользовательские профайлы в системе меню

Тип профайла	Описание	Пароль	Ограничить возможности	Специальные права доступа	Начальное меню
Владелец приложения	Владелец всех объектов приложения, которому предоставлены специальные права доступа *ALL. Приложение управления запасами принадлежит пользователю OWNIC.	*NONE	Не применимо	В соответствии с требованиями приложения	Не применимо
Пользователь приложения ¹	Пример профайла для стандартного пользователя системы меню	Да	*YES	Нет	MENU1
Профайл запросов	Служит для предоставления доступа к библиотекам при обработке запросов	*NONE	Не применимо	Нет	Не применимо
¹ Все создаваемые запросы сохраняются в текущей библиотеке, указанной в пользовательском профайле приложения. В качестве программы обработки нажатия клавиши Attention применяется программа *ASSIST, что дает пользователям возможность применять основные системные функции.					

Таблица 126. Объекты, применяемые в системе меню

Имя объекта	Владелец	Общие права доступа	Частные права доступа	Дополнительные сведения
MENU1 в библиотеке QGPL	См. примечания	*EXCLUDE	*USE для всех пользователей, которым разрешено работать с меню	Меню находится в библиотеке QGPL, поскольку у пользователей нет прав доступа к библиотекам приложений

Таблица 126. Объекты, применяемые в системе меню (продолжение)

Имя объекта	Владелец	Общие права доступа	Частные права доступа	Дополнительные сведения
Программа ICSTART в QGPL	OWNIC	*EXCLUDE	*USE для пользователей, которым разрешено работать с приложением Управление запасами	Создается с параметром USRPRF(*OWNER) для принятия прав доступа OWNIC
Программа QRYSTART в QGPL	QRYUSR	*EXCLUDE	*USE для пользователей, которым разрешено создавать или запускать запросы	Создается с параметром USRPRF(*OWNER) для принятия прав доступа QRYUSR
ITEMLIB	OWNIC	*EXCLUDE	Пользователю QRYUSR предоставлены права доступа *USE	
ICPGMLIB	OWNIC	*EXCLUDE		
Файлы в ITEMLIB, с которыми можно работать с помощью Query	OWNIC	*USE		
Файлы в ITEMLIB, с которыми нельзя работать с помощью Query	OWNIC	*EXCLUDE		
Программы в ICPGMLIB	OWNIC	*USE		
Примечание: Для работы с объектами, которые применяются в нескольких приложениях, можно создать отдельный пользовательский профайл.				

Когда пользователь USERA выбирает опцию 1 (Управление запасами) в меню MENU1, запускается программа ICSTART. Программа принимает права доступа OWNIC, получая права доступа *ALL ко всем объектам управления запасами в ITEMLIB и программам в ICPGMLIB. В связи с этим пользователь USERA может вносить изменения в файлы управления запасами с помощью опций меню ICMENU.

После того как пользователь USERA завершает работу с меню ICMENU и возвращается к MENU1, библиотеки ITEMLIB и ICPGMLIB удаляются из списка библиотек USERA, а программа ICSTART - из стека вызовов. Профайл USERA более не обладает принятыми правами доступа.

При выборе пользователем USERA опции 3 (Query) в меню MENU1 запускается программа QRYSTART. Программа принимает права доступа QRYUSR, получая права доступа *USE к библиотеке ITEMLIB. Файлы, к которым может обращаться пользователь USERA, определяются общими правами доступа к файлам в библиотеке ITEMLIB.

Этот способ позволяет максимально сократить количество частных прав доступа и обеспечивает высокую производительность операций проверки прав доступа:

- Для объектов в библиотеках приложений не задаются частные права доступа. При работе с некоторыми функциями приложений достаточно общих прав доступа. При работе с остальными функциями применяются права доступа владельца. В разделе “Пример 8: Принятые права доступа без частных прав доступа” на стр. 201 описаны этапы проверки прав доступа.
- Для доступа к файлам во время обработки запросов применяются общие права доступа. Особые права доступа к библиотеке ITEMLIB есть только у профайла QRYUSR.
- По умолчанию все программы запросов помещаются в текущую библиотеку пользователя. Эта библиотека должна принадлежать пользователю, и у него должны быть права доступа *ALL.
- Отдельным пользователям необходимы только права доступа к MENU1, ICSTART и QRYSTART.

При использовании данного способа необходимо принять во внимание следующие факторы риска:

- У пользователя USERA есть права доступа *ALL ко всем объектам управления запасами, с которыми он может работать через ICMENU. Убедитесь, что с помощью этого меню нельзя получить доступ к командной строке или запрещенным функциям удаления и обновления.
- Многие средства поддержки принятия решений позволяют работать с командной строкой. Для предотвращения доступа к нежелательным функциям необходимо ограничить возможности профайла QRYUSR и не предоставлять ему специальных прав доступа.

Понятия, связанные с данным

“Планирование защиты файлов” на стр. 248

Как правило, наиболее ценная информация хранится в файлах базы данных системы. С помощью средств защиты ресурсов можно запрещать и разрешать различным пользователям просмотр, изменение и удаление файлов.

Игнорирование принятых прав доступа

При применении принятых прав доступа в проектировании меню пользователю необходимо перейти в начальное меню. Для того чтобы пользователи могли запускать запросы как с помощью начального меню, так и с помощью меню приложений, настройте программу QRYSTART для игнорирования принятых прав доступа.

На рис. 39 показано меню приложения, содержащее программу QRYSTART:



Рисунок 39. Пример меню приложения с запросом

Права доступа для программы QRYSTART совпадают с описанными в разделе Табл. 126 на стр. 243. При создании программы запрещается принятие прав доступа (параметр USEADPAUT равен *NO), чтобы принятые права доступа предыдущих программ из стека игнорировались.

Ниже приведено сравнение стеков вызова при запуске пользователем USERA программы Query из меню MENU1 (см. рис. 36 на стр. 242) и меню ICMENU:

Стек вызова при запуске Query из MENU1

- MENU1 (принятые права доступа отсутствуют)
- QRYSTART (приняты права доступа QRYUSR)

Стек вызова при запуске Query из ICMENU

- MENU1 (принятые права доступа отсутствуют)
- ICMENU (приняты права доступа OWNIC)
- QRYSTART (приняты права доступа QRYUSR)

Программа QRYSTART с параметром USEADPAUT(*NO) не применяет права доступа программ, ранее занесенных в стек. Это позволяет пользователю USERA запускать запросы с помощью ICMENU, не получая возможность удалять и изменять файлы, поскольку программа QRYSTART не принимает права доступа OWNIC.

Когда пользователь USERA завершает обработку запроса и возвращается в меню ICMENU, принятые права доступа снова вступают в силу. Принятые права доступа игнорируются только во время работы программы QRYSTART.

Если для программы QRYSTART заданы общие права доступа *USE, то в качестве дополнительной меры защиты следует указать параметр USEADPAUT(*NO). Это позволит предотвратить запуск программы QRYSTART и применение запрещенных функций с использованием принятых прав доступа.

Описанный прием используется и для меню вопросов (рис. 34 на стр. 241) компании JKL Toys, поскольку это меню можно открыть из нескольких меню, расположенных в разных библиотеках приложений. При этом принимаются права доступа QRYUSR, а все другие принятые права доступа в стеке вызова игнорируются.

Понятия, связанные с данным

“Программы, игнорирующие принятые права доступа” на стр. 160

Указать, будет ли программа использовать принятые права доступа, можно с помощью параметра (USEADPAUT).

Ссылки, связанные с данной

“Блок-схема 8: Проверка принятых прав доступа” на стр. 191

Если проверка прав доступа пользователя показала, что пользователю предоставлены недостаточные права доступа, то система проверяет принятые права доступа.

Информация, связанная с данной

Сценарии для HTTP Server

Системный запрос, меню

С помощью функции Системный запрос пользователь может прервать выполнение текущего задания и перейти в меню Системный запрос. Меню Системный запрос позволяет просмотреть или отправить сообщение, перейти к другому заданию или завершить выполнение текущего задания. Меню Системный запрос поставляется с общими правами доступа *USE, что может быть угрозой для защиты системы.

Для того чтобы запретить пользователям применять это меню, проще всего запретить доступ к группе панелей QGMNSYSR:

- Для того чтобы запретить отдельным пользователям открывать меню Системный запрос, установите для этих пользователей права доступа *EXCLUDE:

```
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +  
           OBJTYPE(*PNLGRP) +  
           USER(USERA) AUT(*EXCLUDE)
```

- Для того чтобы запретить большинству пользователей открывать меню Системный запрос, аннулируйте общие права доступа и предоставьте права доступа *USE отдельным пользователям:

```
RVKOBJAUT OBJ(QSYS/QGMNSYSR) +  
           OBJTYPE(*PNLGRP) +  
           USER(*PUBLIC) AUT(*ALL)  
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +  
           OBJTYPE(*PNLGRP) +  
           USER(USERA) AUT(*USE)
```

Некоторые команды меню Системный запрос перечислены в сообщении CPX2313 из файла сообщений QCPFMMSG. Команды уточнены именем библиотеки из сообщения CPX2373. Значения в сообщении CPX2373 для каждой команды - это *NLVLIBL или *SYSTEM. Потенциально злоумышленник может изменить команды меню Системный запрос с помощью команды Переопределить файл сообщений (OVRMSGF).

При каждом нажатии клавиши System Request система автоматически изменяет текущий пользовательский профайл задания на начальный пользовательский профайл задания. Это делается для того, чтобы у пользователя не было никаких дополнительных прав доступа в меню Системный запрос или в программе выхода Presystem Request Program. По окончании выполнения функции Системный запрос система восстанавливает пользовательский профайл задания, существовавший до нажатия клавиши System Request.

Вы можете предотвратить доступ пользователей к отдельным опциям меню Системный запрос, запретив доступ к соответствующим командам. В таблице Табл. 127 на стр. 247 перечислены команды, связанные с опциями меню:

Таблица 127. Опции меню Системный запрос и связанные с ними команды

Опция	Команда
1	Перейти ко второму заданию (TFRSECJOB)
2	Завершить запрос (ENDRQS)
3	Показать задание (DSPJOB)
4	Показать сообщение (DSPMSG)
5	Отправить сообщение (SNDMSG)
6	Показать сообщение (DSPMSG)
7	Показать пользователя рабочей станции (DSPWSUSR)
10	Запустить Системный запрос в предыдущей системе (TFRPASTHR). (См. примечание ниже.)
11	Перейти к предыдущей системе (TFRPASTHR). (См. примечание ниже.)
12	Показать опции эмуляции 3270 (См. примечание ниже.)
13	Запустить Системный запрос в исходной системе (TFRPASTHR). (См. примечание ниже.)
14	Перейти к исходной системе (TFRPASTHR). (См. примечание ниже.)
15	Перейти к конечной системе (TFRPASTHR). (См. примечание ниже.)
80	Отключить задание (DSCJOB)
90	Выйти из системы (SIGNOFF)

Notes:

- Опции 10, 11, 13, 14 и 15 будут показаны только в том случае, если для удаленного входа в систему дисплейной станции использовалась команда Начать удаленный вход в систему (STRPASTHR). Опции 10, 13 и 14 отображаются только в целевой системе.
- Опция 12 будет показана только в том случае, если активна эмуляция 3270.
- Для некоторых опций в среде System/36 действуют определенные ограничения.

Например, для того чтобы запретить пользователям переход к альтернативному интерактивному заданию, необходимо аннулировать общие права доступа к команде Перейти ко второму заданию (TFRSECJOB) и предоставить права доступа только отдельным пользователям:

```
RVKOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(USERA) AUT(*USE)
```

При выборе пользователем опции, к которой у него нет прав доступа, появляется соответствующее сообщение.

Если пользователям необходимо запретить запуск всех команд из меню Системный запрос, разрешив при этом запускать команды в определенное время (например, при выходе из системы), то можно создать программу на CL, принимающую права доступа пользователя с соответствующими правами доступа и запускающая команду.

Планирование защиты команд

Система поставляется с такой конфигурацией защиты команд, которая соответствует требованиям большинства заказчиков. Некоторые команды разрешено запускать только системному администратору. Для запуска других команд необходимы специальные права доступа, такие как *SAVSYS. Однако большинство команд разрешено запускать всем пользователям системы. Вы можете изменить права доступа к командам в соответствии со своими требованиями к защите.

Например, можно запретить большинству пользователей системы применять средства связи. Для всех команд, работающих с объектами средств связи, таких как CHGCTLxxx, CHGLINxxx и CHGDEVxxx, можно установить общие права доступа *EXCLUDE.

Для того чтобы разрешить пользователям запускать определенные команды, можно задать для этих команд права доступа к объектам. Все команды системы относятся к типу объектов *CMD. Доступ к ним можно предоставить всем пользователям (с помощью общих прав доступа) или отдельным пользователям. Для запуска команды пользователю необходимы права доступа *USE к этой команде. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 перечислены все команды, которые поставляются с общими правами доступа *EXCLUDE.

Если применяется библиотека System/38, то необходимо запретить пользователям доступ к командам из этой библиотеки, требующим защиты. Можно запретить доступ и ко всей библиотеке. Если в системе применяется одна или несколько версий лицензионной программы i5/OS для различных национальных языков, то дополнительно необходимо запретить доступ к командам из библиотек QSYSxxx.

Еще одной эффективной мерой защиты является изменение значений по умолчанию для команд. Это можно сделать с помощью команды Изменить значение по умолчанию для команды (CHGCMDDFT).

Планирование защиты файлов

Как правило, наиболее ценная информация хранится в файлах базы данных системы. С помощью средств защиты ресурсов можно запрещать и разрешать различным пользователям просмотр, изменение и удаление файлов.

Если пользователям необходимы разные права доступа к файлам в разных ситуациях, воспользуйтесь принятыми правами доступа.

Рекомендуется вести в системе реестр пользователей, которым предоставлены права доступа к файлам, содержащим важные данные. Если применяются права доступа групп и списки прав доступа, необходимо отслеживать как пользователей, обращающихся к файлам с применением этих прав доступа, так и пользователей, которым предоставлены свои права доступа к файлам. При использовании принятых прав доступа можно составить список программ, принимающих права доступа отдельного пользователя. Для этого предназначена команда Показать принимающие программы (DSPPGMADP).

С помощью функции ведения журнала системы можно отслеживать операции с файлами, содержащими важные данные. Несмотря на то, что журналы в основном применяются для восстановления информации, их можно использовать и как инструменты защиты. Журнал содержит информацию о том, какие пользователи обращались к файлу и какие операции при этом были выполнены. С помощью команды Показать журнал (DSPJRN) можно регулярно просматривать записи журнала.

Ссылки, связанные с данной

“Применение принятых прав доступа при разработке меню” на стр. 242

Предоставление доступа к средствам поддержки принятия решений, таким как Query/400, предъявляет дополнительные требования к организации защиты. Средства защиты ресурсов не позволяют предоставлять пользователю разные права доступа к файлу в различных ситуациях. Тем не менее, используя принятые права доступа можно настроить такие права доступа, которые необходимы в конкретной ситуации.

Защита логических файлов

Средства защиты ресурсов системы позволяют настроить защиту отдельных полей файлов. Для защиты отдельных полей и записей файла можно использовать и логические файлы.

Логические файлы позволяют указывать наборы *записей*, к которым могут обращаться пользователи (с помощью операций выбора и исключения). Это позволяет запретить отдельным пользователям доступ к

некоторым типам записей. Логические файлы позволяют указывать наборы *полей*, к которым разрешено обращаться отдельным пользователям. Это позволяет запретить отдельным пользователям доступ к некоторым типам полей в записях.

Логический файл не содержит данных. Он задает логическое представление одного или нескольких физических файлов, в которых хранятся данные. Для доступа к информации в логическом файле необходимы права доступа к логическому файлу и к связанным с ним физическим файлам.

На рис. 40 приведен пример физического файла и три разных логических файла, связанных с физическим файлом.

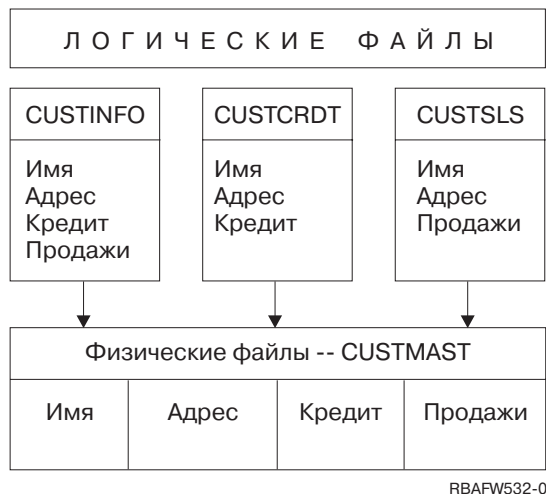


Рисунок 40. Защита данных с помощью логических файлов

Сотрудникам отдела продаж (профайл группы DPTSM) разрешено просматривать все поля, но запрещено изменять максимальную сумму кредита. Сотрудникам отдела дебиторской задолженности (профайл группы DPTAR) разрешено просматривать все поля, но запрещено изменять объем продаж. Для физического файла заданы следующие права доступа:

Таблица 128. Пример физического файла: Файл CUSTMAST

Права доступа	Пользователи: *PUBLIC
Права доступа к объекту	
*OBJOPR	
*OBJMGT	
*OBJEXIST	
*OBJALTER	
*OBJREF	
Права доступа к данным	
*READ	X
*ADD	X
*UPD	X
*DLT	X
*EXECUTE	X
*EXCLUDE	

Всем пользователям должны быть предоставлены права доступа к данным, но не операционные права доступа к физическому файлу CUSTMAST. Общие права доступа не позволяют обращаться к файлу CUSTMAST напрямую, поскольку для того чтобы открыть этот файл, необходимы права доступа *OBJOPR. Общие права доступа предоставляют все права доступа к данным логического файла.

Ниже указаны права доступа к логическому файлу:

```

Показать права доступа к объекту
Объект . . . . . : CUSTINFO Владелец . . . . . : OWNAR
Библиотека . . . . : CUSTLIB Основная группа . . . : *NONE
Тип объекта . . . . : *FILE ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. : *NONE

Профайл      Группа      Права доступа
*PUBLIC

```

```

Показать права доступа к объекту
Объект . . . . . : CUSTCRDT Владелец . . . . . : OWNAR
Библиотека . . . . : CUSTLIB Основная группа . . . : DPTAR
Тип объекта . . . . : *FILE ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. : *NONE

Профайл      Группа      Права доступа
DPTAR
*PUBLIC

```

```

Показать права доступа к объекту
Объект . . . . . : CUSTSLS Владелец . . . . . : OWNSM
Библиотека . . . . : CUSTLIB Основная группа . . . : DPTSM
Тип объекта . . . . : *FILE ASP . . . . . : *SYSBAS
Объект защищен списком прав доступа . . . . .
. : *NONE

Профайл      Группа      Права доступа
DPTSM
*PUBLIC

```

При применении данной схемы защиты можно не выбирать в качестве основной группы логического файла такой профайл группы, как DPTSM. Тем не менее, применение прав доступа основной группы позволяет не выполнять проверку частных прав доступа как пользователя, обращающегося к файлу, так и группы пользователя. В разделе “Пример 2: Применение прав доступа основной группы” на стр. 196 приведен пример того, как применение прав доступа основной группы влияет на процесс проверки прав доступа.

Права доступа к данным для логических файлов можно задавать в лицензионной программе i5/OS, начиная с выпуска V3R1. Когда логический файл выпуска до V3R1 восстанавливается в системе V3R1 или более поздней, система преобразует логические файлы при первом обращении к ним. При этом предоставляются все права доступа к данным.

Для защиты данных с помощью логических файлов выполните следующие действия:

- Предоставьте все права доступа к данным связанных физических файлов.
- Аннулируйте права доступа *OBJOPR к физическим файлам. Это позволит запретить пользователям напрямую обращаться к физическим файлам.
- Предоставьте необходимые права доступа к данным логических файлов. Аннулируйте все ненужные права доступа.
- Предоставьте права доступа *OBJOPR к логическим файлам.

Информация, связанная с данной

DB2 Universal Database для iSeries

Переопределение файлов

Команды переопределения позволяют использовать в программе другой файл с аналогичным форматом.

Рассмотрим ситуацию, когда программа приложения Контракты и цены в компании JKL Toys сохраняет информацию о ценах в рабочем файле перед изменением цен. Пользователь, которому разрешено работать с командной строкой, может перехватить конфиденциальные сведения с помощью команды переопределения, указав в качестве рабочего файл, расположенный в библиотеке, находящейся под управлением пользователя.

Для того чтобы предотвратить такую ситуацию, перед запуском программы следует вызвать команды переопределения с параметром SECURE(*YES). Тем самым эти файлы будут защищены от влияния любых ранее вызванных команд переопределения файлов. Параметр SECURE(*NO) не защищает файлы от влияния команд переопределения файлов. Их значения можно переопределить, вызвав команду переопределения файлов.

Защита файлов и SQL

Будьте осторожны при применении команды CL с принятыми правами доступа для запуска SQL или программы Query Manager. Эти программы для запуска запросов позволяют пользователям указывать имена файлов. Это позволяет пользователям обращаться ко всем файлам, доступ к которым разрешен принятыми правами доступа профайла.

В языке структурных запросов (SQL) для отслеживания файлов базы данных и их взаимосвязи применяются файлы перекрестных ссылок. Совокупность этих файлов называется каталогом SQL. Для каталога SQL заданы общие права доступа *READ. Это позволяет всем пользователям, которым предоставлены права на работу с интерфейсом SQL, просматривать имена и текстовые описания всех файлов системы. При работе с каталогом SQL проверяется наличие тех прав доступа, которые необходимы для работы с содержимым файлов баз данных.

Планирование профайлов групп

Профайл группы - это эффективный инструмент для управления несколькими профайлами пользователей с одинаковыми требованиями к защите. Можно либо специально создать профайл группы, либо преобразовать в профайл группы один из существующих профайлов. Профайлы групп позволяют повысить эффективность управления правами доступа и сократить число записей о частных правах доступа к отдельным объектам.

С помощью файлов групп можно быстро реагировать на изменение требований задания к защите и изменять состав группы. Например, если с приложением разрешено работать только сотрудникам одного отдела, для этого отдела можно создать профайл группы. При появлении новых сотрудников или уходе сотрудников из отдела в их пользовательских профайлах будет меняться лишь поле профайла группы. Это намного удобнее, чем удалять отдельные права доступа из пользовательских профайлов.

Профайл группы - это особый тип пользовательского профайла. Профайл пользователя считается профайлом группы в следующих случаях:

- Если он указан в качестве профайла группы в другом профайле

- Если ему присвоен идентификационный номер группы (gid).

Например:

1. Создайте профайл GRPIC:
CRTUSRPRF GRPIC
2. После создания это будет обычный профайл, а не профайл группы.
3. Укажите профайл GRPIC в качестве профайла группы в другом профайле группы:
CHGUSRPRF USERA GRPPRF(GRPC)
4. После выполнения этой команды система будет работать с профайлом GRPIC как с профайлом группы и присвоит ему gid.

Понятия, связанные с данным

“Профайлы групп” на стр. 5

Профайл группы - это особый тип пользовательского профайла. Если требуется предоставить одинаковые права доступа нескольким пользователям, то с помощью профайла группы вы можете сделать это за один прием.

Замечания об основной группе объектов

Для любого объекта системы можно задать основную группу. Если основная группа объекта является первой группой большинства пользователей этого объекта, то, задав права доступа для основной группы, можно повысить производительность системы.

Как правило, группа пользователей работает с информацией определенного типа, такой как сведения о заказчиках. Пользователям этой группы необходимы более широкие права доступа к этой информации, чем остальным пользователям системы. С помощью прав доступа основной группы можно настроить такую схему защиты без ущерба для производительности операций проверки прав доступа.

Задачи, связанные с данной

“Пример 2: Применение прав доступа основной группы” на стр. 196

В это примере описано применение прав доступа основной группы.

Особенности профайлов нескольких групп

Профайлы групп позволяют повысить эффективность управления правами доступа и сократить число записей о частных правах доступа к отдельным объектам. Тем не менее, неправильное применение таких профайлов может привести к увеличению времени проверки прав доступа. В этом разделе приведены рекомендации по работе с профайлами нескольких групп.

Пользователь может входить не более чем в 16 групп: первую группу (параметр GRPPRF пользовательского профайла) и 15 дополнительных групп (параметр SUPGRPPRF пользовательского профайла).

Ниже приведены некоторые рекомендации по работе с несколькими профайлами групп:

- При использовании нескольких групп рекомендуется применять права доступа основной группы, не указывая частные права доступа к объектам.
- Тщательно спланируйте последовательность добавления пользователя в группы. Первая группа пользователя должна соответствовать тем объектам, с которыми пользователь чаще всего работает. Для примера предположим, что пользователь WAGNERB регулярно работает с запасами и периодически - с заказами. Профайл, необходимый для доступа к запасам (DPTIC), следует указать в качестве первой группы WAGNERB. В качестве первой дополнительной группы необходимо указать профайл, который служит для работы с заказами (DPTOE).

Примечание: Порядок присвоения частных прав доступа не влияет на производительность операций проверки прав доступа.

- Если в системе будет применяться несколько групп, ознакомьтесь с описанием процедуры проверки прав доступа, приведенным в разделе “Как система проверяет права доступа” на стр. 177. Необходимо четко

понимать, каким образом применение нескольких групп в сочетании с другими способами предоставления прав доступа, такими как списки, может повлиять на производительность системы.

Накопление специальных прав доступа для участников профайла группы

Пользователю, входящему в несколько групп, предоставляются объединенные специальные права доступа.

Входящие в группу пользователи могут использовать специальные права доступа, предоставленные этой группе. Если пользовательский профайл входит в состав нескольких групп, то помимо собственных специальных прав доступа он обладает специальными правами доступа всех этих групп. Пользователю, входящему в несколько групп, предоставляются объединенные специальные права доступа. Для примера предположим, что у профайла GROUP1 есть специальные права доступа *JOBCTL, у профайла GROUP3 - права *AUDIT, а у профайла GROUP16 - права *IOSYSCFG. Пользовательский профайл, входящий в состав этих трех групп, будет обладать специальными правами доступа *JOBCTL, *AUDIT и *IOSYSCFG.

Примечание: Если входящему в группу пользователю принадлежит программа, она принимает только права доступа владельца. Права доступа группы владельца не принимаются.

Применение профайла пользователя в качестве профайла группы

Профайлы групп рекомендуется создавать специально, а не получать путем преобразования существующих профайлов пользователей.

Если права доступа пользователя полностью совпадают с правами, которые необходимо предоставить группе пользователей, то быстрее преобразовать его профайл в профайл группы. Однако в будущем применение профайла пользователя в качестве профайла группы может привести к возникновению следующих проблем:

- При изменении сферы ответственности пользователя, профайл которого используется в качестве профайла группы, вам потребуется выбрать другой профайл в качестве профайла группы, изменить права доступа и изменить принадлежность объектов.
- Все пользователи, входящие в группу, будут автоматически получать права доступа ко всем объектам, создаваемым с помощью профайла группы. Пользователь, профайл которого применяется в качестве профайла группы, должен будет явно запрещать доступ другим пользователям группы к тем объектам, которые он планирует использовать в частном порядке.

Профайлы групп рекомендуется планировать заблаговременно. Для этого можно создать профайлы групп с паролем *NONE. Если после завершения работы приложения будет обнаружено, что определенному пользователю предоставлены права доступа, которые можно предоставить группе, выполните следующие действия:

1. Создайте профайл группы.
2. С помощью команды GRTUSRAUT установите для профайла группы права доступа пользователя.
3. Удалите частные права доступа пользователя, поскольку они ему больше не понадобятся. Используйте команды RVKOBJAUT или EDTOBJAUT.

Сравнение профайлов групп и списков прав доступа

Профайлы групп позволяют упростить управление пользовательскими профайлами с одинаковыми требованиями к защите. Списки прав доступа предназначены для защиты объектов со схожими требованиями.

В Табл. 129 подробно описаны особенности этих способов защиты.

Таблица 129. Сравнение списка прав доступа и профайла группы

Сравнительная характеристика	Список прав доступа	Задан профайл группы
Применяется для защиты нескольких объектов	Да	Да

Таблица 129. Сравнение списка прав доступа и профайла группы (продолжение)

Сравнительная характеристика	Список прав доступа	Задан профайл группы
Может применяться несколькими пользователями	Да	Да
Частные права доступа переопределяют все остальные права доступа	Да	Да
Права доступа предоставляются каждому пользователю по отдельности	Да	Нет
Одинаковые права доступа для всех объектов	Да	Нет
Для защиты объектов может применяться несколько экземпляров	Нет	Да
Права доступа можно задать при создании объекта	Да	Да ¹
Защита объектов всех типов	Нет	Да
Удаление связи с объектом при удалении объекта	Да	Да
Сохранение связи с объектом при сохранении объекта	Да	Да ²
¹ При создании объекта можно указать права доступа для профайла группы, задав значение параметра GRPAUT в профайле создающего объект пользователя.		
² При сохранении объекта сохраняются права доступа основной группы. Частные права доступа группы сохраняются при указании для команды сохранения параметра PVTAUT(*YES).		

Для списка прав доступа для пункта "Права доступа можно задать при создании объекта":

- Для того чтобы присвоить список прав доступа объекту библиотеки, укажите AUT(*LIBCRTAUT) в команде CRTxxxx и CRTAUT (имя_списка_прав_доступа) для библиотеки. Для некоторых объектов, например контрольных списков, значение *LIBCRTAUT в команде CRT указывать нельзя.
- Для того чтобы присвоить список прав доступа объекту каталога, укажите значение *INDIR в параметрах DTAAUT и OBJAUT команды MKDIR. В этом случае список прав доступа будет защищать и родительский, и вновь созданный каталоги. Система не допускает указания произвольного списка прав доступа при создании объекта.

Планирование защиты от программистов

Работа программистов представляет определенную угрозу безопасности системы. Знания, которыми обладают программисты, позволяют им найти слабые места в защите системы и обойти защиту.

Программист может обойти защиту для получения данных, необходимых для тестирования. Кроме того, он может повлиять на обычную процедуру распределения ресурсов в системе, чтобы повысить производительность своих заданий за счет заданий других пользователей. Часто программисты рассматривают средства защиты как препятствие для выполнения своих действий, таких как тестирование приложений. Однако предоставление программистам широких прав доступа к объектам системы противоречит основному принципу защиты, заключающемуся в разделении обязанностей. Кроме того, это дает возможность программистам устанавливать запрещенные программы.

Ниже приведены рекомендации по настройке среды для разработчиков приложений:

- Не предоставляйте программистам все специальные права доступа. Предоставляйте им только те специальные права доступа, которые необходимы для решения задач, связанных с разработкой программ.
- Не используйте пользовательский профайл QPGMR в качестве профайла группы для программистов.
- Применяйте тестовые библиотеки и запретите программистам доступ к рабочим библиотекам.
- Создайте библиотеки для программистов. Скопируйте в них необходимые для тестирования рабочие данные с помощью программы, принимающей права доступа.
- Если в системе недостаточно интерактивной производительности, то измените команды создания программ таким образом, чтобы они выполнялись только в пакетном режиме:

```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
```

- Перед переносом приложений или обновлений программ из тестовых библиотек в рабочие библиотеки проверяйте их безопасность.
- На этапе разработки приложения используйте профайл группы. Все прикладные программы должны принадлежать профайлу группы. Включите разработчиков приложений в эту группу и укажите в профайлах разработчиков, что владельцем всех создаваемых объектов будет профайл группы (параметр OWNER(*GRPPRF)). При переходе программиста от одного проекта к другому можно изменить профайл группы в профайле программиста. Дополнительная информация приведена в разделе “Групповая принадлежность объектов” на стр. 150.
- Разработайте план изменения принадлежности приложений при их переносе в рабочую среду. Для того чтобы иметь возможность контролировать все изменения рабочего приложения, объекты приложения (в том числе программы) должны принадлежать пользовательскому профайлу приложения.

Объекты приложения не должны принадлежать программистам, поскольку в противном случае программисты получат неконтролируемый доступ к этим объектам в рабочей среде. Приложение может принадлежать как профайлу пользователя, ответственного за приложение, так и профайлу, специально созданному в качестве владельца приложения.

Управление исходными файлами

Для защиты информации в системе необходимо обеспечить защиту исходных файлов.

Исходные файлы позволяют обеспечивать целостность системы. Кроме того, они являются ценным активом компании, если эта компания разработала или приобрела приложения заказчика. Исходные файлы необходимо защищать так же, как и остальные важные файлы системы. Рекомендуется поместить исходные файлы в отдельные библиотеки и ограничить права на обновление этих файлов и их перемещение в рабочую среду.

При создании исходного файла в системе для него по умолчанию устанавливаются общие права доступа *CHANGE, благодаря чему любой пользователь может обновить любой элемент исходного файла. Удалять и добавлять элементы по умолчанию разрешено только владельцу исходного файла и пользователю со специальными правами доступа *ALLOBJ. В большинстве случаев устанавливаемые по умолчанию права доступа к исходным физическим файлам требуется изменить. Для добавления новых элементов в исходный файл у разработчика приложений должны запрашиваться права доступа *OBJMGT. В качестве общих прав доступа рекомендуется указать значение *USE или *EXCLUDE, если исходные файлы не расположены в библиотеке, доступ к которой жестко контролируется.

Защита файлов class и jar Java в интегрированной файловой системе

Для запуска программ Java необходимы права доступа на чтение (*R) ко всем файлам class и jar Java, а также права доступа на выполнение (*X) к каждому каталогу в пути к файлам class и jar Java. Если вы применяете файлы class Java и файлы jar в интегрированной файловой системе, то их нужно защитить с помощью обычных прав доступа к объектам.

Для того чтобы защитить файлы Java, настройте защиту каталогов пути и файлов с помощью команды CHGAUT с атрибутами прав доступа к объектам. Пользователю могут понадобиться права на чтение (*R) к файлам классов Java и файлам jar, чтобы запускать программу на языке Java. Эти права доступа пользователь может получить из общих прав доступа файла или из частных прав доступа. Настроить частные права доступа для группы пользователей удобно с помощью списка прав доступа. Не предоставляйте права на запись (*W) никаким пользователям, за исключением тех, кому разрешено изменять файл.

Проконтролировать правильность файлов из CLASSPATH, используемых выполняющимся приложением на языке Java, можно с помощью параметра Проверить уровень защиты CLASSPATH (CHKPATH) команды RUNJVA. Значение CHKPATH(*SECURE) позволяет запретить выполнение программы Java, если для каталогов в CLASSPATH с открытым доступом на запись возникают предупреждения.

Планирование защиты от системных программистов и менеджеров

Для защиты файлов в системе можно ограничить права доступа, предоставляемые системным программистам и менеджерам.

В большинстве случаев обслуживанием системы занимается специальный сотрудник организации. Он отслеживает использование системных ресурсов, в том числе дисковой памяти, и время от времени проверяет, удаляют ли пользователи ненужные объекты с диска. Системным программистам необходимы широкие права доступа для отслеживания всех объектов системы. Однако им не нужен доступ к содержимому этих объектов.

Для того чтобы предоставить системным программистам доступ к группе команд меню рекомендуется использовать принятые права доступа, а не предоставлять специальные права доступа пользовательскому профайлу.

Например, можно возложить обязанность создания и изменения пользовательских профайлов сотрудниками Ивану и Елене, не предоставляя им специальные права доступа. Это достигается следующими действиями.

1. Напишите команду или программу, вызывающую команду CRT/CHGUSRPRF.
2. Эта команда или программа должна принимать профайл, способный выполнять операции создания и изменения.
3. Предоставьте Ивану и Елене право на выполнение этой программы.

Тогда они смогут выполнять задачу только с помощью этого приложения.

Работа с контрольными списками

Контрольные списки позволяют приложениям обеспечить защищенное хранение идентификационной информации пользователей.

Например, на сервере Internet Connection Server (ICS) контрольные списки применяются для поддержки пользователей Internet. ICS может выполнять простую идентификацию перед предоставлением Web-страницы. При простой идентификации пользователи должны предоставить некоторые идентификационные данные, такие как пароль, PIN или номер счета. Имя пользователя и идентификационные данные могут храниться в защищенном контрольном списке. Сервер ICS может использовать для идентификации пользователей информацию из контрольного списка вместо имени и пароля пользователя System i.

Пользователю Internet можно запретить или разрешить доступ к системе с Web-сервера. У такого пользователя не будет прав доступа к ресурсам System i и прав доступа для входа в систему и запуска заданий. Для пользователей Internet не создается пользовательский профайл System i.

Для создания и удаления контрольного списка предназначены команды CL Создать контрольный список (CRTVLDL) и Удалить контрольный список (DLTVLDL). Помимо этих команд предусмотрены интерфейсы прикладных программ (API), которые позволяют применять в приложениях функции добавления, изменения, удаления, проверки (идентификации) и поиска записей контрольных списков.

Объекты контрольного списка могут применяться во всех приложениях. Например, если для работы с приложением необходим пароль, то пароли приложения можно хранить в контрольном списке, а не в файле базы данных. Приложение может проверять зашифрованные пароли пользователей с помощью API контрольного списка. Так как контрольный список зашифрован, этот способ безопаснее, чем проверка пароля только с помощью приложения.

Идентификационную информацию можно хранить в виде, допускающем расшифровку. Если у пользователя есть необходимые права доступа, то он может получить эти данные в расшифрованном виде.

Ссылки, связанные с данной

“Сохранить идентификационные данные на сервере (QRETSVRSEC)” на стр. 34
Системное значение Сохранить идентификационные данные на сервере (QRETSVRSEC) позволяет определить, следует ли сохранять на хосте зашифрованную идентификационную информацию, связанную с пользовательскими профайлами или записями контрольного списка (*VLDL). Пароли пользовательских профайлов System i в данном случае не сохраняются.

Информация, связанная с данной

Интерфейсы прикладных программ

Ограничение доступа к функциям программ

Ограничение доступа к функциям программы позволяет предоставить доступ к приложению, его компонентам или отдельным функциям программы только некоторым пользователям.

Эта функция не предоставляет возможностей, аналогичных средствам защиты ресурсов. Ограничение доступа к функциям программ не позволяет запретить пользователям доступ к ресурсам (таким как файл или программа) с помощью других интерфейсов. Для проверки функции выполняются следующие действия.

- Регистрация функции
- Получение информации о функциях
- Указание пользователей, которым разрешено и запрещено работать с функциями
- Проверка, есть ли у пользователя права доступа для применения функции

Ограничение доступа к функциям программ позволяет API выполнять следующие задачи: Для применения этой функции в приложении его разработчику необходимо зарегистрировать функции при установке приложения. Зарегистрированная функция соответствует блоку кода конкретной функции в приложении. При выполнении приложения перед запуском блока кода вызывается API, проверяющий наличие прав доступа к функции, связанной с этим блоком. Если пользователю разрешено применять зарегистрированную функцию, этот блок кода запускается. В противном случае код не запускается.

Системный администратор указывает, каким пользователям разрешен доступ к функции, а каким запрещен. Для управления доступом к функции программы администратор может использовать команду Работа с информацией о правах доступа к функции (WRKFCNUSG) или функцию Администрирование приложений Навигатора System i Navigator.

Информация, связанная с данной

Администрирование приложений

Глава 8. Резервное копирование и восстановление информации защиты

Сохранение информации о защите не менее важно, чем сохранение данных. В некоторых случаях может возникнуть необходимость восстановления пользовательских профайлов, прав доступа к объектам и данным системы. Если информация о защите не сохранялась, то пользовательские профайлы и права доступа к объектам придется восстанавливать вручную. Это может занять существенное время, привести к возникновению ошибок и риску нарушения безопасности.

В этом разделе вы найдете информацию по следующим вопросам:

- Сохранение и восстановление информации о защите
- Влияние защиты на сохранение и восстановление объектов
- Вопросы безопасности, связанные со специальными правами доступа *SAVSYS

Для правильного планирования процедур резервного копирования и восстановления необходимо хорошо понимать принципы хранения, сохранения и восстановления информации.

В Табл. 130 приведены команды для сохранения и восстановления информации о защите. В последующих частях этого раздела вопросы сохранения и восстановления информации о защите обсуждаются более подробно.

Таблица 130. Сохранение и восстановление информации о защите

Сохраненная или восстановленная информация о защите	Использованные команды сохранения и восстановления					
	SAVSECDTA SAVSYS	SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG	RSTUSRPRF	RSTOBJ RSTLIB RSTDLO RSTCFG	RSTAUT	RSTDFROBJ
Пользовательские профайлы	X		X			
Принадлежность объекта ¹		X		X		X
Основная группа ¹		X		X		X
Общие права доступа ¹		X		X		X
Частные права доступа ³	X	X	X	X	X	X
Списки прав доступа	X		X			
Владельцы прав доступа	X		X			
Связь между списком прав доступа и владельцами прав доступа		X		X		
Значение уровня контроля объектов		X		X		
Информация о регистрации функций ² .		X		X		
Информация об использовании функций	X		X		X	
Контрольные списки		X		X		
Записи идентификации сервера	X		X			

Таблица 130. Сохранение и восстановление информации о защите (продолжение)

Сохраненная или восстановленная информация о защите	Использованные команды сохранения и восстановления					
	SAVSECDTA SAVSYS	SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG	RSTUSRPRF	RSTOBJ RSTLIB RSTDLO RSTCFG	RSTAUT	RSTDFROBJ
1	Команды SAVSECDTA, SAVSYS и RSTUSRPRF выполняют сохранение и восстановление принадлежности, основной группы, прав доступа основной группы и общих прав доступа объектов следующих типов: Пользовательский профайл (*USRPRF), Список прав доступа(*AUTL) и Владелец прав доступа (*AUTHLR).					
2	Сохраняется и восстанавливается объект QUSEXRGOBJ типа *EXITRG из библиотеки QUSRSYS.					
3	Частные права доступа для всех объектов сохраняются командой SAVSECDTA. RSTUSRPRF восстанавливает всю информацию, требуемую для восстановления частных прав доступа. Частные права доступа восстанавливаются командой RSTAUT. Частные права доступа для отдельных объектов восстанавливаются командами SAV, SAVLIB, SAVOBJ и SAVCHGOBJ. Частные права доступа для отдельных объектов можно восстановить командами RST, RSTLIB и RSTOBJ, если они были сохранены командой сохранения.					

Информация, связанная с данной

Создание резервных копий и восстановление



Резервное копирование и восстановление PDF

Хранение информации о защите

Для правильного планирования процедур резервного копирования и восстановления необходимо хорошо понимать принципы сохранения и восстановления информации.

Информация о защите может храниться вместе с объектами, пользовательскими профайлами или списками прав доступа:

Информация о правах доступа, сохраняемая вместе с объектом:

- Общие права доступа
- Имя владельца
- Права доступа владельца к объекту
- Имя основной группы
- Права доступа основной группы к объекту
- Имя списка прав доступа
- Значение уровня контроля объектов
- Наличие частных прав доступа
- Наличие частных прав доступа, более ограниченных, чем общие

Информация о правах доступа, сохраняемая вместе с объектом:

- *Информация заголовка:*
 - Атрибуты пользовательского профайла, задаваемые в окне Создать пользовательский профайл.
 - Идентификатор пользователя и идентификатор группы.
- *Информация о частных правах доступа:*
 - Частные права доступа к объектам. Сюда также входят частные права доступа к спискам прав доступа.
- *Информация о принадлежности:*
 - Список объектов, принадлежащих профайлу.

- Для каждого такого объекта хранится также список пользователей, имеющих частные права доступа к этому объекту.
- *Информация об основной группе:*
 - Список объектов, для которых профайл является основной группой.
- *Информация о контроле:*
 - Значение уровня контроля действий
 - Значение уровня контроля объектов
- *Информация об использовании функций:*
 - Параметры использования зарегистрированных функций.
- | • *Информация об идентификации сервера:*
 - | – Записи идентификации сервера.

Информация о правах доступа, хранимая вместе со списком прав доступа:

- Обычная информация о правах доступа, хранимая с любым объектом; например, общие права доступа и принадлежность.
- Список всех объектов, защищенных списком прав доступа.

Понятия, связанные с данным

“Дополнительная информация, связанная с пользовательскими профайлами” на стр. 120

В этом разделе обсуждаются частные права доступа, информация о принадлежности объекта и информация об объекте главной группы, относящиеся к пользовательскому профайлу.

Сохранение информации о защите

Хранение информации о защите на внешнем носителе организовано иначе, чем в системе. При сохранении пользовательских профайлов хранящаяся вместе с ними информация о частных правах доступа форматируется в виде таблицы прав доступа.

Таблица прав доступа создается и сохраняется для каждого профайла, обладающего частными правами доступа. При наличии в системе большого числа частных прав доступа такое форматирование и сохранение может занимать очень много времени.

Хранение информации о защите на носителе данных:

Информация о правах доступа, сохраняемая вместе с объектом:

- Общие права доступа
- Имя владельца
- Права доступа владельца к объекту
- Имя основной группы
- Права доступа основной группы к объекту
- Имя списка прав доступа
- Права доступа на уровне поля
- Значение уровня контроля объектов
- Наличие частных прав доступа
- Наличие частных прав доступа, более ограниченных, чем общие
- | • Частные права доступа к объекту сохраняются при указании для команды SAVxxx параметра
- | PVTAUT(*YES).

Информация о правах доступа, хранимая вместе со списком прав доступа:

- Обычная информация о правах доступа, хранимая с любым объектом; например, общие права доступа, основная группа и принадлежность.

Информация о правах доступа, сохраняемая вместе с пользовательским профайлом:

- Атрибуты пользовательского профайла, задаваемые в окне Создать пользовательский профайл.
- Прочая информация приложения, связанная с пользовательским профайлом. Например:
 - Записи идентификации сервера
 - Записи пользовательской информации о приложении, добавленные с помощью API Обновить пользовательскую информацию о приложении (QsyUpdateUserApplicationInfo)

Таблица прав доступа, сохраняемая вместе с пользовательским профайлом:

- Каждая запись соответствует частным правам доступа пользовательского профайла, включая параметры использования зарегистрированных функций.

Информация о регистрации функций, сохраняемая вместе с объектом QUSEXRGOBJ:

- Для сохранения информации о зарегистрированных функциях можно сохранить объект QUSEXRGOBJ типа *EXITRG в библиотеке QUSRSYS.

Восстановление информации о защите

Восстановление системы после сбоя часто включает в себя восстановление данных и связанной с ними информации о защите.

Обычная последовательность действий при восстановлении системы выглядит так:

1. Восстановление пользовательских профайлов и списков прав доступа (RSTUSRPRF USRPRF(*ALL)).
2. Восстановление объектов (RSTCFG, RSTLIB, RSTOBJ, RSTDLO или RST).
3. Восстановление частных прав доступа к объектам (RSTAUT).

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе Глава 10, “Лицензия на исходный код и отказ от обязательств”, на стр. 325.

Информация, связанная с данной



Резервное копирование и восстановление

Восстановление пользовательских профайлов

При восстановлении пользовательского профайла в него могут быть внесены некоторые изменения.

Это возможно в следующих случаях:

- Если профайлы восстанавливаются по отдельности (RSTUSRPRF USRPRF(*ALL) не указано), не указан параметр SECDDTA(*PWDGRP), а восстанавливаемый профайл не существует в системе. В этом случае следующим параметрам будет присвоено значение *NONE:
 - Имя профайла группы (GRPPRF)
 - Пароль (PASSWORD)
 - Пароль документа (DOCPWD)
 - Профайлы дополнительных групп (SUPGRPPRF)

Пароли программных продуктов также изменятся на *NONE, поэтому они будут недействительны после восстановления пользовательского профайла, ранее не существовавшего в системе.

- Если профайлы восстанавливаются по отдельности (RSTUSRPRF USRPRF(*ALL) не указано), не указан параметр SECDDTA(*PWDGRP), а восстанавливаемый профайл уже существует в системе, то его пароль, пароль документов и групповой профайл останутся без изменений.

Пользовательские профайлы можно восстанавливать и по отдельности, с помощью информации о пароле и основной группе, хранящейся на носителе данных. Для этого при выполнении команды RSTUSRPRF необходимо указать параметр SECDDTA(*PWDGRP). Для восстановления пароля и информации о группе

пользовательского профайла необходимы права доступа *ALLOBJ и *SECADM. Если параметр SECDDTA(*PWDGRP) не указан, то после восстановления пользовательского профайла, существующего в системе, пароли программных продуктов, восстановленные вместе с ним, будут недействительны.

- Если восстанавливаются сразу все пользовательские профайлы, то все параметры профайлов, существующих в системе, включая пароль, будут восстановлены с носителя данных.

Внимание:

1. Если пользовательские профайлы были сохранены в системе, уровень пароля в которой (системное значение QPWDLVL) отличается от уровня пароля в системе восстановления, то некоторые пароли могут оказаться недействительными. Допустим, например, что пользовательский профайл сохранен в системе с уровнем пароля 2 и его пароль имеет вид "Это мой пароль". Такой пароль окажется недопустимым в системе с уровнем пароля 0 или 1.
2. Записывайте пароль системного администратора (QSECOFR) для каждой сохраненной версии информации о защите, чтобы обеспечить возможность входа в систему в случае, если потребуется полное восстановление.

Пароль профайла QSECOFR можно сбросить с помощью DST (Специальных сервисных средств).

- Если восстанавливаемый профайл уже существует в системе, то его uid или gid при восстановлении не изменятся.
- Если профайл не существует в системе, то его uid и gid будут восстановлены с носителя данных. Если в системе уже существуют такие uid или gid, то система создаст новые значения и отправит пользователю сообщение (CPI3810).
- При восстановлении профайлов в системе с уровнем защиты 30 и выше у восстанавливаемых профайлов могут быть аннулированы специальные права доступа *ALLOBJ. Это происходит в следующих случаях:
 - Профайл был сохранен в другой системе, а пользователь, выполняющий команду RSTUSRPRF, не имеет специальных прав доступа *ALLOBJ и *SECADM.
 - Профайл был сохранен в этой же системе с уровнем защиты 10 или 20.

Внимание: Для того чтобы определить, в какой системе восстанавливаются объекты, сравнивается серийный номер, присвоенный системе восстановления, и сохраненный на носителе данных.

Для следующих профайлов, поставляемых IBM, специальные права доступа *ALLOBJ не аннулируются:

- QSYS (системный пользовательский профайл)
- QSECOFR (пользовательский профайл системного администратора)
- QLPAUTO (пользовательский профайл автоматической установки лицензионных программ)
- QLPINSTALL (установка лицензионных программ), пользовательский профайл

Информация, связанная с данной

Сброс пароля профайла i5/OS QSECOFR

Восстановление объектов

При восстановлении объекта система использует информацию о правах доступа, сохраненную вместе с этим объектом. В этом разделе описаны правила, применяемые к информации о правах доступа при восстановлении объектов.

При этом параметры защиты объекта обрабатываются следующим образом:

Принадлежность объекта:

- Если профайл, которому принадлежит объект, существует в системе, то восстановленный объект будет принадлежать ему.
- Если профайл, которому принадлежит объект, отсутствует в системе, то объект передается во владение пользовательскому профайлу QDFTOWN (владелец по умолчанию).

- Если объект уже существует в системе, а его владелец не совпадает с указанным на носителе, то объект будет восстановлен только при указании параметра ALWOBJDIF(*ALL) или ALWOBJDIF(*OWNER). При этом владельцем восстановленного объекта будет профайл, указанный в системе.
- В разделе “Восстановление программ” на стр. 266 приведены дополнительные сведения о восстановлении программ.

Основная группа:

Если объект не существует в системе:

- Если профайл основной группы объекта существует в системе, то для этого объекта будут восстановлены права доступа и значение основной группы.
- Если профайл основной группы объекта не существует в системе, то:
 - Восстановленный объект не будет иметь основной группы.
 - Будут заданы права доступа основной группы *NONE.

Если восстанавливаемый объект уже существует в системе, то его основная группа в процессе восстановления не изменится.

Общие права доступа:

- Если восстанавливаемый объект не существует в системе, то общие права доступа к нему будут такими же, как у сохраненного объекта.
- Если при восстановлении замещается объект, уже существующий в системе, то общие права доступа к нему останутся без изменений. Информация об общих правах доступа, указанная в сохраненной версии объекта, при этом не используется.
- При восстановлении объектов в библиотеке права доступа CRTAUT этой библиотеки не применяются.

Список прав доступа:

- Если объект (не документ и не папка) уже существует в системе и связан со списком прав доступа, то результат зависит от значения параметра ALWOBJDIF:
 - Если указано ALWOBJDIF(*NONE), то списки прав доступа существующего и сохраненного объекта должны совпадать. В противном случае объект не будет восстановлен.
 - Если указано ALWOBJDIF(*ALL) или ALWOBJDIF(*AUTL), то объект будет восстановлен. В этом случае он будет связан с тем же списком прав доступа, что и уже существующий объект.
- Если восстанавливается документ или папка, уже существующие в системе, то используется список прав доступа, связанный с существующим объектом. Список прав доступа сохраненного документа или папки не используется.
- Если список прав доступа отсутствует в системе, то объект будет восстановлен без связи со списком прав доступа, а его общие права доступа будут изменены на *EXCLUDE.
- Если объект восстанавливается в той же системе, в которой он был сохранен, то он будет заново связан со своим списком прав доступа.
- Если объект восстанавливается в системе, отличной от той, в которой он был сохранен, то он может быть связан или не связан со списком прав доступа, в зависимости от параметра ALWOBJDIF:
 - Если указано ALWOBJDIF(*ALL) или ALWOBJDIF(*AUTL), то объект связывается со списком прав доступа.
 - Если указано ALWOBJDIF(*NONE), то объект не связывается со списком прав доступа, а его общие права доступа изменяются на *EXCLUDE.

Частные права доступа:

- Частные права доступа сохраняются в пользовательском профайле при указании для команды SAVxxx параметра PVTAUT(*YES).

- Если у пользовательского профайла были права доступа к объекту, то восстановление этого объекта на них, как правило, не влияет. Однако восстановление определенных типов программ может привести к тому, что частные права доступа будут аннулированы.
- | • Если объект удаляется из системы, то частные прав доступа к этому объекту будут аннулированы. При удалении объекта частные права доступа к нему удаляются из всех профайлов. Если затем объект восстанавливается из сохраненной версии, то частные права доступа будут восстановлены, если при сохранении был указан параметр PVTAUT(*YES).
- | • Если частные права доступа не были сохранены с объектом, то их можно восстановить с помощью команды Восстановить права доступа (RSTAUT). Обычная последовательность действий при восстановлении выглядит так:
- | 1. Восстановление пользовательских профайлов
- | 2. Восстановление объектов
- | 3. Восстановление прав доступа

Контроль за объектом:

- Если восстанавливается объект, не существующий в системе, то значение контроля этого объекта будет соответствовать сохраненному.
- Если при восстановлении замещается объект, уже существующий в системе, то значение контроля этого объекта останется без изменений. Значение OBJAUD сохраненного объекта при этом не восстанавливается.
- Если восстанавливается библиотека или каталог, не существующие в системе, то значение контроля за созданием объекта или каталога (CRTOBJAUD) для этой библиотеки или каталога также будет восстановлено.
- Если восстанавливаемая библиотека или каталог уже существуют в системе, то значение CRTOBJAUD восстановлено не будет. Вместо него будет применяться значение CRTOBJAUD существующей библиотеки или каталога.

Владелец прав доступа:

- Если восстанавливается файл, с именем которого и с библиотекой, в которую он восстанавливается, связан владелец прав доступа, то файл будет связан с этим владельцем прав доступа.
- Информация о правах доступа, связанная с владельцем прав доступа, заменит информацию об общих правах доступа и владельце, сохраненную вместе с файлом.

Объекты пользовательского домена:

Системы разрешают размещение объектов пользовательского домена (*USRSPC, *USRIDX и *USRQ) только в библиотеках, указанных в системном значении QALWUSRDMN. Если после сохранения объекта пользовательского домена типа *USRSPC, *USRIDX или *USRQ библиотека этого объекта была удалена из системного значения QALWUSRDMN, то он будет восстановлен как объект системного домена.

Информация о регистрации функций:

Для восстановления информации о регистрации функций необходимо восстановить объект QUSEXRGOBJ типа *EXITRG в библиотеке QUSRSYS. При этом будут восстановлены все зарегистрированные функции. Связанная с функциями информация об использовании восстанавливается вместе с пользовательскими профайлами и правами доступа.

Регистрация приложений, применяющих сертификаты:

Информация о регистрации приложений, использующих сертификаты, восстанавливается вместе с объектом QUSEXRGOBJ типа *EXITRG в библиотеке QUSRSYS. При этом восстанавливаются все

зарегистрированные приложения. Для установления связей между приложениями и их сертификатами необходимо восстановить объект QYCDCERTI типа *USRIDX в библиотеке QUSRSYS.

Понятия, связанные с данным

“Восстановление программ”

Восстановление в системе программ, полученных из неизвестного источника, представляет собой потенциальную опасность. В этом разделе приведена информация об особенностях восстановления программ.

“Восстановление списков прав доступа” на стр. 268

Восстановить отдельно взятый список прав доступа невозможно. При восстановлении списка прав доступа его принадлежность и права доступа определяются так же, как при восстановлении любых других объектов.

Восстановление прав доступа

Восстановив информацию о защите, следует заново создать частные права доступа. При восстановлении пользовательского профайла, имеющего таблицу прав доступа, эта таблица будет также восстановлена.

Команда Восстановить права доступа (RSTAUT) создает частные права доступа пользовательского профайла в соответствии с информацией, указанной в таблице прав доступа. Для каждой записи о частных правах доступа, указанной в таблице, выполняется операция предоставления прав доступа. Этот процесс может оказаться достаточно долгим, особенно если права доступа восстанавливаются для большого числа профайлов, а таблицы прав доступа имеют много записей.

Команды RSTUSRPRF и RSTAUT можно запустить для отдельного профайла, списка профайлов, профайлов с именем, отвечающем заданному шаблону, или для всех профайлов. Система ищет профайлы, подлежащие восстановлению, на носителе данных или в файле сохранения, созданном командой SAVSECDTA или SAVSYS, либо API QSRVAVO.

| Если частные права доступа сохраняются вместе с объектами, то их также можно восстановить вместе с объектами. Это рекомендуется при сохранении и восстановлении небольшого числа объектов, но не всей системы.

Восстановление прав доступа к полям:

Действия, необходимые для восстановления частных прав доступа к полям файлов базы данных, не существующих в системе:

- Восстановить или создать необходимые пользовательские профайлы.
- Восстановить файлы.
- Запустить команду Восстановить права доступа (RSTAUT).

Частные права доступа к полям будут полностью восстановлены только после восстановления частных прав доступа к самим объектам.

Восстановление программ

Восстановление в системе программ, полученных из неизвестного источника, представляет собой потенциальную опасность. В этом разделе приведена информация об особенностях восстановления программ.

Программы могут выполнять операции, не отвечающие предъявляемым требованиям безопасности. В особенности это касается программ, содержащих команды с ограниченным доступом, программ, принимающих права доступа своего владельца, и программ, подвергнутых изменениям. В том числе это относится к объектам типа *PGM, *SRVPGM, *MODULE и *CRQD. Предотвратить восстановление объектов этих типов можно с помощью системных значений QVFYOBJRST, QFRCCVNRST и QALWOBJRST.

Для защиты программ система использует контрольное значение. Это значение сохраняется вместе с программой и вычисляется заново при ее восстановлении. Действия системы определяются значением параметра ALWOBJDIF команды восстановления и системным значением преобразования при восстановлении (QFRCCVNRST).

Примечание: Программы содержат информацию, позволяющую при необходимости заново создать программу во время восстановления. Информация, необходимая для воссоздания программы, остается с ней даже когда в программе отсутствует информация наблюдаемости. Если при восстановлении программы обнаружена ошибка контрольного значения, то программа создается заново для того, чтобы исправить эту ошибку.

Восстановление программ, принимающих права доступа владельца:

При восстановлении программ, принимающих права доступа своих владельцев, принадлежность и права доступа к программе могут измениться. Это возможно в следующих случаях:

- Пользовательский профайл, выполняющий восстановление, должен быть владельцем программы или иметь специальные права доступа *ALLOBJ и *SECADM.
- Пользовательский профайл, выполняющий восстановление, получает права на восстановление в следующих ситуациях:
 - Он является владельцем программы.
 - Он является членом группового профайла, которому принадлежит программа (если нет частных права доступа к программе).
 - Он имеет специальные права доступа *ALLOBJ и *SECADM.
 - Он является членом группового профайла, имеющего специальные права доступа *ALLOBJ и *SECADM.
 - Он работает с принятыми правами доступа, удовлетворяющими одному из вышеперечисленных условий.
- Если профайл, выполняющий восстановление, не имеет необходимых прав доступа, то все общие и частные права доступа к программе будут аннулированы, а общие права доступа примут значение *EXCLUDE.
- Если профайл, которому принадлежит программа, отсутствует в системе, то программа передается пользовательскому профайлу QDFTOWN (владелец по умолчанию). Общие права доступа меняются на *EXCLUDE, а список прав доступа удаляется.

Понятия, связанные с данным

“Восстановление объектов” на стр. 263

При восстановлении объекта система использует информацию о правах доступа, сохраненную вместе с этим объектом. В этом разделе описаны правила, применяемые к информации о правах доступа при восстановлении объектов.

Ссылки, связанные с данной

“Системные значения восстановления, связанные с защитой” на стр. 44

В этом разделе описаны системные значения, связанные с восстановлением операционной системы i5/OS.

Восстановление лицензионных программ

В этом разделе описано восстановление лицензионных программ в системе.

Команда Восстановить лицензионную программу (RSTLICPGM) используется для установки в системе программ IBM. С ее помощью также можно устанавливать программы независимых производителей, созданные с помощью лицензионной программы IBM System Manager для i5/OS.

Изначально команду RSTLICPGM могут использовать только пользователи со специальными правами доступа *ALLOBJ. Процедура RSTLICPGM вызывает программу выхода для установки программ, поставляемых не IBM.

В целях обеспечения безопасности программа выхода не должна запускаться из профайла со специальными правами доступа *ALLOBJ. Вместо прямого запуска команды RSTLICPGM пользователем со специальными правами доступа *ALLOBJ следует применять программу, принимающую такие права доступа.

Приведем пример, иллюстрирующий эту процедуру. Допустим, что необходимо требуется установить названием CPAPP с помощью команды RSTLICPGM.

1. Сначала необходимо создать профайл с правами доступа, достаточными для успешной установки программы. Не следует предоставлять этому профайлу права доступа *ALLOBJ. В этом примере пользовательский профайл называется OWNCP.
2. Затем следует написать программу для установки приложения. Присвоим этой программе имя CPINST:

Примечание: Используя приведенные примеры программ, вы обязуетесь соблюдать требования, изложенные в разделе Глава 10, “Лицензия на исходный код и отказ от обязательств”, на стр. 325.

```
PGM
RSTLICPGM CPAPP
ENDPGM
```

3. Создайте программу CPINST таким образом, чтобы она принимала права доступа пользователя со специальными правами доступа *ALLOBJ (например QSECOFR), и предоставьте профайлу OWNCP права на использование этой программы:

```
CRTCLPGM QGPL/CPINST USRPRF(*OWNER) +
AUT(*EXCLUDE)GRTOBJAUT OBJ(CPINST) OBJTYP(*PGM) +
USER(OWNCP) AUT(*USE)
```

4. Войдите в систему под именем OWNCP и запустите CPINST. В момент выполнения команды RSTLICPGM программой CPINST вы обладаете правами системного администратора (QSECOFR). При запуске программы выхода, осуществляющей установку программ CPAPP, эти права доступа аннулируются. Поэтому все программы, вызываемые программой выхода, будут выполняться с правами доступа OWNCP.

Восстановление списков прав доступа

Восстановить отдельно взятый список прав доступа невозможно. При восстановлении списка прав доступа его принадлежность и права доступа определяются так же, как при восстановлении любых других объектов.

Связь между списками прав доступа и объектами устанавливается только в том случае, если объекты восстанавливаются после списков прав доступа. Частные права доступа пользователя к списку можно восстановить с помощью команды RSTAUT.

Списки прав доступа сохраняются с помощью команд SAVSECDTA или SAVSYS. Восстановить списки прав доступа можно командой

```
RSTUSRPRF USRPRF(*ALL)
```

Восстановление поврежденного списка прав доступа

В случае повреждения списка прав доступа доступ к объекту будет разрешен только пользователям со специальными правами доступа *ALLOBJ.

Восстановление поврежденного списка прав доступа выполняется в два этапа:

1. Восстановление пользователей и их прав доступа в списке прав доступа.
2. Восстановление связи списка прав доступа с объектами.

Эти действия должны выполняться пользователем со специальными правами доступа *ALLOBJ.

Понятия, связанные с данным

“Восстановление объектов” на стр. 263

При восстановлении объекта система использует информацию о правах доступа, сохраненную вместе с этим объектом. В этом разделе описаны правила, применяемые к информации о правах доступа при восстановлении объектов.

Восстановление списка прав доступа

В этом разделе приведены инструкции по восстановлению списка прав доступа.

Если права доступа пользователей к списку прав доступа известны, то восстановите список прав доступа, как указано далее.

1. Удалите список прав доступа.
2. Снова создайте список прав доступа.
3. Добавьте в него всех известных пользователей.

Если права доступа пользователей неизвестны, то список вместе с записями можно восстановить с последней версии магнитной ленты SAVSYS или SAVECDTA. Для этого выполните следующие действия:

1. Удалите поврежденный список прав доступа с помощью команды Удалить список прав доступа (DLTAUTL).
2. Восстановите список прав доступа, восстановив пользовательские профайлы:
RSTUSRPRF USRPRF (*ALL)
3. Восстановите частные права доступа пользователей к списку с помощью команды RSTAUT.

Эта процедура восстанавливает значения пользовательских профайлов с носителя сохранения.

Дополнительная информация о восстановлении пользовательских профайлов с носителя данных приведена в разделе “Восстановление пользовательских профайлов” на стр. 262.

Восстановление связи объектов со списком прав доступа

В этом разделе приведены инструкции по восстановлению связи объектов со списком прав доступа.

После удаления поврежденного списка прав доступа объекты, защищенные им, необходимо добавить в новый список. Для этого выполните следующие действия:

1. Найдите объекты, которые были связаны с поврежденным списком прав доступа, с помощью команды Восстановить память (RCLSTG). Процедура восстановления памяти связывает эти объекты со списком прав доступа QRCLAUTL.
2. Для просмотра объектов, связанных со списком прав доступа QRCLAUTL, воспользуйтесь командой Показать объекты списка прав доступа (DSPAUTOBJ).
3. Свяжите каждый объект с нужным списком прав доступа с помощью команды Предоставить права доступа к объекту (GRTOBJAUT):

```
GRTOBJAUT  
OBJ(имя_библиотеки/имя_объекта) +  
  OBJTYPE(тип_объекта) +  
  AUTL(имя_списка_прав_доступа)
```

Если со списком QRCLAUTL связано слишком много объектов, то создайте файл базы данных, запустив команду DSPAUTOBJ с параметром OUTPUT(*OUTFILE). Затем можно написать программу на CL, которая будет выполнять команду GRTOBJAUT для каждого объекта из этого файла.

Восстановление операционной системы

При выполнении IPL в ручном режиме в меню IPL или установка операционной системы можно выбрать опцию установки операционной системы. Функция специальных сервисных средств (DST) дает возможность запрашивать пароль DST у всех пользователей, выбирающих эту опцию. Эту возможность можно использовать для защиты от восстановления несанкционированной копии операционной системы.

Для защиты от установки операционной системы выполните следующие действия:

1. Выполните IPL в режиме Manual.
2. В меню IPL или Установка системы выберите DST.
3. В меню DST выберите опцию Работа со средой DST.
4. Выберите опцию Изменить пароль DST.
5. Выберите Изменение защиты от установки операционной системы.
6. Выберите опцию 1 (защищать).
7. Нажимайте F3 (Выход) до тех пор, пока вы не попадете в меню IPL или установка системы.
8. Завершите IPL и верните переключатель режима в положение Normal.

Notes:

1. Если вы больше не нуждаетесь в защите от установки операционной системы, выполните те же действия и выберите опцию 2 (не защищать).
2. Предотвратить установку операционной системы можно также, установив переключатель режима в положение Normal, и вытащив ключ.

Специальные права доступа *SAVSYS

Для сохранения и восстановления объекта необходимы права доступа *OBJEXIST к этому объекту или специальные права доступа *SAVSYS. Пользователь со специальными правами доступа *SAVSYS может сохранять или восстанавливать объекты, не обладая дополнительными правами доступа к ним.

Специальные права доступа *SAVSYS дают пользователю возможность сохранять объекты и переносить их в другую систему для восстановления, а также создавать дампы носителя для просмотра данных. Они также позволяют пользователю сохранять объекты и освобождать дисковое пространство, удаляя данные объектов. При сохранении документов пользователь со специальными правами доступа *SAVSYS может также удалять их. При предоставлении пользователям специальных прав доступа *SAVSYS следует соблюдать осторожность.

Контроль операций сохранения и восстановления

Если в значении уровня контроля (системное значение QAUDLVL или параметр AUDLVL пользовательского профайла) указано *SAVRST, то при каждом выполнении операции восстановления создается запись контроля действий. При использовании команд, восстанавливающих большое число объектов, например RSTLIB, запись контроля создается для каждого восстановленного объекта. Это может привести к неполадкам, связанным с размером получателя журнала контроля, особенно если вы восстанавливаете сразу несколько библиотек.

Команда RSTCFG не создает записи контроля для каждого восстановленного объекта. Если вы хотите, чтобы при использовании этой команды запись создавалась, включите контроль объектов для самой этой команды. Тогда запись контроля будет создаваться при каждом запуске этой программы.

Команды, сохраняющие очень большое количество объектов (например SAVSYS, SAVSECDTA, и SAVCFG), не создают отдельных записей для каждого сохраняемого объекта, даже если применяется контроль за этими объектами. Если вы хотите отслеживать их применение, необходимо включить контроль для самих объектов этих команд.

Глава 9. Контроль эффективности защиты системы System i

В этом разделе описаны возможные способы контроля эффективности защиты системы.

Контролировать действия в системе необходимо по следующим причинам:

- Для проверки правильности выбранного плана защиты.
- Для того чтобы убедиться, что средства управления защитой правильно установлены и настроены. Администратор защиты регулярно выполняет соответствующие действия. Кроме того, эти действия могут выполняться, иногда в расширенном варианте, при периодических проверках защиты внутренними или внешними контролерами.
- Для того чтобы убедиться, что конфигурация защиты соответствует текущей системной среде. Ниже приведены примеры изменений среды, которые могут повлиять на защиту системы:
 - Создание новых объектов пользователями
 - Добавление новых пользователей
 - Передача объектов другим владельцам (без изменения прав доступа к объектам)
 - Изменение полномочий пользователей (смена группы)
 - Временное предоставление прав доступа без их своевременного аннулирования
 - Установка новых продуктов
- Для подготовки к выполнению определенной операции: установке нового приложения, повышению уровня защиты или настройке новой сети.

Приведенная в этой главе информация может применяться в любой из этих ситуаций. Выбор объектов для контроля и частота его проведения зависят от размера организации и требований к защите. В этой главе нет рекомендаций по выбору частоты, с которой следует выполнять действия по контролю. Здесь приведены сведения о доступной информации, а также способах ее получения и применения.

Этот раздел состоит из трех частей, содержащих следующую информацию:

- Перечень объектов, действия над которыми можно контролировать.
- Информацию о настройке и применении журнала контроля, предоставляемого системой.
- Информацию о других способах сбора информации о защите в системе.

Контролирование действий заключается, помимо прочего, в применении команд и просмотре журналов и протоколов в System i. Для администратора, выполняющего контроль за действиями, рекомендуется создать отдельный профайл. У этого профайла должны быть специальные права доступа *AUDIT, позволяющие изменять параметры контроля. Для выполнения некоторых задач контроля, описанных в этом разделе, необходим пользовательский профайл со специальными правами доступа *ALLOBJ и *SECADM. По окончании периода контроля пароль профайла администратора контроля следует изменить на *NONE.

Понятия, связанные с данным

“Журнал контроля за действиями” на стр. 6

Журнал контроля за действиями повышает эффективность защиты системы.

Справочная таблица для системных администраторов и администраторов контроля

Эта справочная таблица применяется для планирования защиты системы и контроля.

Во время планирования выберите те пункты, которые отвечают вашим требованиям к защите. При контроле эффективности защиты эта таблица позволяет оценить действующие средства защиты системы и, при необходимости, принять решение о применении дополнительных средств защиты.

Таблица может рассматриваться как краткий обзор информации, содержащейся в этих разделах. Она содержит краткое описание команд, системных значений и параметров, с помощью которых можно настроить контроль, а также перечень записей, которые заносятся в журнал QAUDJRN при возникновении контролируемого события. Подробные сведения приведены в соответствующих разделах.

Физическая защита

Справочная таблица контроля физической защиты применяется для планирования или контроля физической защиты системы.

Примечание: В разделе Планирование и настройки защиты системы приведена полная информация по физической защите продукта System i.

Ниже приведена справочная таблица для планирования физической защиты системы:

- ___ • Системный блок и консоль находятся в надежном месте.
- ___ • Носитель резервной копии защищен от повреждения и хищения.
- ___ • С помощью ключа на блоке процессора установлен режим Secure или Auto. Ключи хранятся отдельно, в хорошо защищенном месте. Дополнительная информация о переключателе режимов приведена в разделе Планирование физической защиты системного блока.
- ___ • Доступ к рабочим станциям и консоли, расположенным в общедоступных местах, ограничен. С помощью команды DSPOBJAUT можно проверить, кому предоставлены права доступа *CHANGE к рабочим станциям. Попытки входа в систему на рабочих станциях с ограниченным доступом фиксируются в записях AF журнала контроля, в которых поле типа объекта содержит значение *DEV.D.
- ___ • Пользователям со специальными правами доступа *ALLOBJ или *SERVICE разрешено входить в систему только с некоторых рабочих станций. Убедитесь, что системное значение QLMTSECOFR равно 1. Для того чтобы узнать, предоставлены ли профайлу QSECOFR права доступа *CHANGE, вызовите команду DSPOBJAUT для устройства.

Системные значения

Настройка параметров контроля системных значений позволяет отслеживать их изменения.

- Системные значения защиты заданы в соответствии с приведенными рекомендациями. Для того чтобы напечатать системные значения, введите: WRKSYSVAL *SEC OUTPUT (*PRINT). Необходимо контролировать два наиболее важных системных значения:
 - QSECURITY, значение которого не должно быть меньше 40.
 - QMAXSIGN, значение которого не должно быть больше 5.

Примечание: Если функция контроля активна, при любом изменении системного значения в журнал QAUDJRN заносится запись SV.

- С помощью команды Показать атрибуты защиты (DSPSECA) проверьте текущее и ожидающее значения QSECURITY (уровень защиты) и QPWDLV (уровень пароля) и текущее значение системы, связанной с защитой (индикатор возможности изменять значения).
- Периодически проверяйте правильность параметров контроля системных значений. Это особенно важно при изменении среды системы, например, при установке новых приложений или подключении к сети.

Пользовательские профайлы, поставляемые IBM

Задачи контроля пользовательских профайлов, поставляемых IBM, выполняются посредством проверки их паролей.

- Пароль пользовательского профайла QSECOFR был изменен.

Этот профайл поставляется с паролем QSECOFR, чтобы вы могли войти в систему для выполнения установки. Этот пароль должен быть изменен во время первого входа в систему; кроме того, его необходимо периодически изменять в процессе дальнейшей работы.

Для того чтобы проверить, изменен ли пароль, введите команду DSPAUTUSR и найдите дату изменения пароля QSECOFR. Попробуйте войти в систему с паролем по умолчанию.

- Изменены пароли IBM для Специальных сервисных средств (DST).

ИД пользователей сервисных средств не отображаются в выводе команды DSPAUTUSR. Для того чтобы убедиться в том, что ИД и пароли пользователей были изменены, запустите DST и введите значения по умолчанию.

- За исключением QSECOFR, не применяйте поставляемые IBM пользовательские профайлы для входа в систему.

Данные профайлы являются владельцами объектов или используются для запуска определенных системных функций. С помощью команды DSPAUTUSR проверьте, установлен ли пароль *NONE для поставляемых IBM пользовательских профайлов, перечисленных в разделе Приложение В, “Пользовательские профайлы, поставляемые IBM”, на стр. 337, кроме QSECOFR.

Понятия, связанные с данным

“IBM, поставляемые пользовательские профайлы” на стр. 133

Некоторые пользовательские профайлы поставляются вместе с программным обеспечением. Такие пользовательские профайлы, поставляемые IBM, являются владельцами объектов многих системных функций. Кроме того, некоторые функции системы выполняются от имени пользовательских профайлов, поставляемых IBM.

“Работа с ИД пользователей сервисных средств” на стр. 135

Появился ряд дополнений и расширений, сделавших применение сервисных средств более простым и удобным.

Ссылки, связанные с данной

Приложение В, “Пользовательские профайлы, поставляемые IBM”, на стр. 337

В этом разделе содержится информация о пользовательских профайлах, поставляемых вместе с системой. Данные профайлы применяются в качестве владельцев объектов при выполнении различных функций системы. Кроме того, некоторые функции системы выполняются от имени пользовательских профайлов, поставляемых IBM.

Контроль паролей

Для защиты системы применяются механизмы контроля паролей.

- Пользователи могут изменять свои собственные пароли.

Возможность выбрать свой пароль позволяет пользователю установить в качестве пароля такое значение, которое он может запомнить, не записывая его. Пользователям должен быть предоставлен доступ к команде CHGPWD или к функции Изменить пароль меню Защита (GO SECURITY).

- В соответствии с рекомендациями по организации защиты предприятия пароль необходимо периодически изменять (обычно через 30-90 дней).

Системное значение QPWDEXPITV должно быть настроено в соответствии с этими рекомендациями.

- Пароли пользовательских профайлов, отличные от системного значения, соответствуют рекомендациям.

Проверьте в пользовательских профайлах значения параметра PWDDEXPITV, отличные от *SYSVAL.

- Установлен запрет на использование тривиальных паролей; для этого применяются системные значения, устанавливающие правила задания паролей, и программа подтверждения паролей.

С помощью команды WRKSYSVAL *SEC проверьте системные значения, имена которых начинается с букв QPWD.

- Для профайлов групп задан пароль *NONE.

С помощью команды DSPAUTUSR проверьте все профайлы групп, у которых есть пароль.

Когда уровень паролей в системе отличен от уровня 3, при изменении пароля пользователем система пытается создать эквивалентный пароль, который применим на других уровнях пароля. Для того чтобы определить, у каких пользовательских профайлов есть пароли, применимые на разных уровнях, введите команду PRTUSRPRF TYPE(*PWLVL).

Примечание: Генерация эквивалентного пароля является оптимальным способом создания пароля, применимого на других уровнях, однако такой пароль может не соответствовать правилам создания паролей, действующим на данном уровне. Например, если на уровне 2 определен пароль BbAaA3x, то система создает эквивалентный пароль BBAAA3X для использования на уровнях 0 и 1. Это будет выполнено даже в том случае, если системное значение QPWDLMTCHR запрещает использовать символ 'A' (QPWDLMTCHR не действует на уровне паролей 2) или системное значение QPWDLMTREP запрещает совпадение соседних символов (поскольку проверка пароля на уровне 2 выполняется с учетом регистра, а на уровне 0 и 1 - без учета регистра символов).

Профайлы пользователей и групп

Для контроля эффективности защиты системы можно проверить профайлы пользователей и групп и их права доступа.

- Для каждого пользователя определен уникальный пользовательский профайл.

Системное значение QLMTDEVSSN должно быть равно 1. Несмотря на то, что при ограничении сеансов каждого пользователя одним устройством совместное использование пользовательских профайлов не запрещено, оно нежелательно.

- Число пользовательских профайлов со специальными правами доступа *ALLOBJ невелико. Эти профайлы не применяются в качестве профайлов групп.

С помощью команды DSPUSRPRF можно узнать, какие специальные права доступа предоставлены пользовательским профайлам, и определить, какие профайлы являются профайлами групп. В разделе “Печать выбранных пользовательских профайлов” на стр. 320 описано, как это можно сделать с помощью запроса и файла вывода.

- В поле *Ограничить возможности* профайлов пользователей, которым должен быть предоставлен доступ только к фиксированному набору меню, указано значение *YES.

В примере из раздела “Печать выбранных пользовательских профайлов” на стр. 320 показано, как определить это значение.

- Доступ программистов к рабочим библиотекам ограничен.

Для того чтобы узнать, какие общие и частные права доступа установлены для рабочих библиотек и наиболее важных объектов из этих библиотек, введите команду DSPOBJAUT. В разделе “Планирование защиты от программистов” на стр. 254 приведена подробная информация о защите и среде программирования.

- При изменении обязанностей сотрудника меняется группа этого сотрудника.

Для проверки членства в группе введите одну из следующих команд:

```
DSPAUTUSR SEQ(*GRPPRF)
DSPUSRPRF имя-профайла *GRPMBR
```

- Профайлам группы следует присваивать имена в соответствии с принятыми соглашениями.

Тогда при просмотре прав доступа вы сможете легко распознать профайл группы.

- Правильно организована структура пользовательских профайлов.

В системе нет пользовательских профайлов с большим числом частных прав доступа. В разделе “Просмотр больших пользовательских профайлов” на стр. 321 обсуждается, как найти в системе большие пользовательские профайлы и проверить их.

- При увольнении или переводе сотрудников они немедленно удаляются из системы.

Регулярно просматривайте вывод команды DSPAUTUSR и проверяйте, что доступ к системе предоставлен только действующим сотрудникам. Для того чтобы проверить, удалены ли пользовательские профайлы уволенных сотрудников, просмотрите записи DO (Удалить объект) в журнале контроля.

- Руководство регулярно проверяет, каким пользователям предоставлен доступ к системе.

Используйте команду DSPAUTUSR для просмотра информации об авторизации пользователей.

- Для неработающих сотрудников установлен пароль *NONE.

С помощью команды DSPAUTUSR убедитесь в том, что для профайлов неработающих сотрудников не заданы пароли.

- Руководство регулярно проверяет, каким пользователям предоставлены специальные права доступа, в особенности права доступа *ALLOBJ, *SAVSYS и *AUDIT.

В примере из раздела “Печать выбранных пользовательских профайлов” на стр. 320 показано, как определить это значение.

Управление доступом

Проверка прав доступа позволяет контролировать защиту информации в системе.

Ниже приведена справочная таблица для контроля проверки прав доступа.

- Владельцы данных понимают, что следует предоставлять доступ только к тем данным, которые действительно необходимы для работы пользователя.
- Владельцы объектов регулярно проверяют права на использование этих объектов, включая общие права доступа.

Команда WRKOBJOWN предоставляет меню для работы с правами доступа ко всем объектам, принадлежащим пользовательскому профайлу.

- Конфиденциальные данные не находятся в свободном доступе. С помощью команды DSPOBJAUT проверьте, какие права доступа предоставлены пользователю *PUBLIC к важным объектам.
- Ограничен доступ к пользовательским профайлам.

Общие права доступа к пользовательским профайлам должны быть равны *EXCLUDE. Это позволяет запретить пользователям передавать на выполнение задания, запускаемые с профайлом другого пользователя.

- Контролируются описания заданий:
 - В описаниях заданий с общими правами доступа *USE или выше задан параметр USER(*RQD). Задание, переданное на выполнение с помощью такого описания задания, должно выполняться с профайлом пользователя, передавшего задание на выполнение.
 - Для описаний заданий, в которых задан пользователь, установлены общие права доступа *EXCLUDE. Права на использование этих описаний заданий предоставлены ограниченному кругу пользователей. Это позволяет запретить большей части пользователей передавать на выполнение задания, применяющие права доступа другого профайла.

Для того чтобы узнать, какие описания заданий есть в системе, введите:

DSPOBJD OBJ(*ALL/*ALL) OBJTYPE(*JOB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)

Для того чтобы проверить значение параметра *Пользователь* в описании задания, введите команду Показать описание задания (DSPJOB). Для того чтобы проверить права доступа к описанию задания, введите команду Показать права доступа к объекту (DSPOBJAUT).

Примечание: Если уровень защиты равен 40 или 50, то для передачи на выполнение задания с помощью описания, в котором указано имя пользовательского профайла, у пользователя должны быть права доступа *USE как к этому описанию задания, так и к указанному в нем пользовательскому профайлу. Попытка передать на выполнение или запланировать задание при отсутствии прав доступа *USE к профайлу, указанному в описании этого задания, на любом уровне защиты приведет к тому, что в журнал контроля будет занесена запись AF с типом нарушения J.

- Пользователям запрещен вход в систему путем нажатия клавиши Enter в меню входа в систему.

Убедитесь в том, что ни в одной записи рабочей станции в описаниях подсистем не указано описание задания, в параметре USER которого задано имя пользовательского профайла.

На уровне защиты 40 и 50 вход в систему по умолчанию запрещен, даже если он разрешен в описании подсистемы. На любом уровне защиты вход в систему по умолчанию с описанием подсистемы, допускающим такой вход в систему, фиксируется в журнале контроля путем добавления записи AF с типом нарушения S.

- Контролируются списки библиотек в прикладных программах, чтобы не допустить добавления в список библиотеки с аналогичной программой перед рабочими библиотеками.

Способы управления списками библиотек обсуждаются в разделе “Списки библиотек” на стр. 218.

- Программы, принимающие права доступа, используются только тогда, когда это необходимо, и тщательно контролируются.

В разделе “Анализ программ, принимающих права доступа” на стр. 322 описано, каким образом может использоваться функция принятия прав доступа.

- Интерфейсы прикладных программ (API) защищены.
- Для того чтобы избежать снижения производительности, применяются эффективные способы защиты объектов.

Несанкционированный доступ

Эта справочная таблица вместе с журналом контроля позволяет отслеживать попытки несанкционированного доступа к информации.

- Если функция контроля активна, то информация о событиях, влияющих на защиту, заносится в журнал контроля за действиями (QAUDJRN).

Для контроля за нарушениями прав доступа используйте следующие системные значения и параметры:

- QAUDCTL должно быть равно *AUDLVL.
- QAUDLVL должно включать значения *PGMFAIL и *AUTFAIL.

Лучший способ отследить попытки несанкционированного доступа к информации заключается в регулярном просмотре записей журнала контроля.

- Системное значение QMAXSIGN ограничивает максимальное число последовательных неудачных попыток входа в систему пятью попытками. Системное значение QMAXSGNACN равно 2 или 3.
- Очередь сообщений QSYSMSG создана и отслеживается.
- Журнал контроля проверяется на наличие записей, свидетельствующих о повторных попытках пользователя войти в систему. (Если при входе в систему у пользователя не было обнаружено необходимых прав доступа, то в журнал контроля заносится запись типа AF.)

- Программам запрещено обращаться к объектам через неподдерживаемые интерфейсы. (Системное значение QSECURITY равно 40 или 50.)
- При входе в систему запрашивается ИД и пароль пользователя.

На уровне защиты 40 и 50 ввод ИД и пароля обязателен. На уровне 20 или 30 следует убедиться, что ни одно из описаний подсистем не содержит запись рабочей станции, использующую описание задания, в котором указано имя пользовательского профайла.

Несанкционированный доступ к программам

Для обнаружения несанкционированных изменений в объектах программ применяется запускается команда Проверить целостность объекта (CHKOBJTG).

- Системное значение QALWOBJRST равно *NONE. Оно запрещает всем пользователям восстанавливать в системе программы, влияющие на защиту.
- Для обнаружения несанкционированных изменений в объектах программ периодически запускается команда Проверить целостность объекта (CHKOBJTG).

Описание команды приведено в разделе “Проверка измененных объектов” на стр. 322.

Средства связи

Приведенная здесь справочная таблица может применяться как для планирования связи в системе, так и для контроля за ее эффективностью.

- Используйте ответный звонок для защиты телефонных соединений.
- Используйте шифрование важных данных.
- Ограничьте удаленный вход в систему. Установлено системное значение QRMTSIGN *FRCSIGNON или применяется программа проверки удаленного входа в систему.
- С помощью сетевых атрибутов JOBACN, PCSACC и DDMACC контролируется доступ к данным из других систем, в том числе с персональных компьютеров. Для сетевого атрибута JOBACN должно быть установлено значение *FILE.

Работа с журналом контроля за действиями

Журнал контроля за действиями - основной источник контрольной информации в системе. В этом разделе обсуждается планирование и настройка контроля за действиями, управление контролем, типы сохраняемой информации и способы ее просмотра.

С помощью функции контроля администратор контроля может собрать информацию о произошедших в системе событиях, повлиявших на ее защиту.

Контроль в системе может вестись на трех уровнях:

- Контроль за всеми пользователями во всей системе.
- Контроль за определенными объектами.
- Контроль за определенными пользователями.

Для настройки параметров контроля используются системные значения, параметры пользовательских профайлов и параметры объектов. В разделе “Планирование контроля за действиями” на стр. 278 приведена подробная информация по этому вопросу.

Если происходит событие, которое влияет на защиту и может быть проконтролировано, система проверяет, выбрали ли вы это событие для контроля. Если да, то в текущий получатель журнала контроля за действиями (журнала QAUDJRN в библиотеке QSYS) добавляется запись.

Если вам необходимо проанализировать данные контроля, собранные в журнале QAUDJRN, вы можете воспользоваться командой Показать журнал (DSPJRN). С помощью этой команды можно записать информацию из журнала QAUDJRN в файл базы данных. Для анализа данных можно использовать прикладную программу или утилиту запросов.

Ссылки, связанные с данной

Приложение F, “Макет записей журнала контроля”, на стр. 593

В этом разделе содержится информация о форматах всех типов записей журнала контроля (QAUDJRN) с кодом T. Для управления этими записями служат значения контроля действий и объектов, определяемые пользователем.

Приложение E, “Работа с объектами и контроль за объектами”, на стр. 527

В этом разделе перечислены операции, которые можно выполнять над объектами системы, и приведена информация о том, какие из этих операций контролируются.

Планирование контроля за действиями

Функцию контроля за действиями применять необязательно. Для настройки контроля за действиями необходимо выполнить определенные операции.

Для того чтобы спланировать контроль в системе, выполните следующие действия:

- Определите, какие события, влияющие на защиту, необходимо регистрировать для всех пользователей системы. Контроль за событиями, влияющими на защиту, называется *контролем действий*.
- Определите, необходим ли дополнительный контроль за определенными пользователями.
- Решите, следует ли контролировать использование определенных объектов в системе.
- Определите, контролировать ли использование объектов всеми или только некоторыми пользователями.

Планирование контроля действий

Для контроля действий используются системные значения QAUDCTL (управление контролем), QAUDLVL (уровень контроля), QAUDLVL2 (расширение уровня контроля), а также параметр AUDLVL (контроль действий) из пользовательских профайлов.

Ниже перечислены функции этих системных значений:

- Системное значение QAUDLVL определяет, какие действия контролируются для всех пользователей в системе.
- Системное значение QAUDLVL2 также определяет, какие действия контролируются для всех пользователей в системе, и используется в том случае, когда применяется более 16 значений контроля.
- Параметр AUDLVL из пользовательского профайла определяет, какие действия контролируются для конкретного пользователя. Значения параметра AUDLVL *дополняют* системные значения QAUDLVL и QAUDLVL2.
- Системное значение QAUDCTL служит для включения и выключения контроля действий.

Список фиксируемых событий зависит от целей защиты и от потенциальных угроз. В “Контроль действий” на стр. 118 описаны возможные значения уровня контроля и рекомендации по их применению. В частности, указано, можно ли указывать значение контроля в системном значении и в параметре пользовательского профайла.

Ссылки, связанные с данной

“Уровень контроля (QAUDLVL)” на стр. 71

Системное значение Уровень контроля (QAUDLVL) совместно с системным значением QAUDLVL2 определяет события, связанные с защитой, которые заносятся в журнал контроля за действиями (QAUDJRN) всех пользователей.

“Расширение уровня контроля (QAUDLVL2)” на стр. 72

Системное значение Расширение уровня контроля (QAUDLVL2) необходимо для применения более шестнадцати значений контроля.

“Контроль действий” на стр. 118

Для каждого пользователя можно указать действия, связанные с защитой, которые следует регистрировать в журнале контроля за действиями. Действия, указанные для отдельных пользователей применяются совместно с действиями, указанными для всех пользователей с помощью системных значений QAUDLVL и QAUDLVL2.

Значения уровня контроля действий:

В этой таблице перечислены возможные значения уровня контроля действий, доступные для системных значений QAUDLVL и QAUDLVL2 и команды CHGUSRAUD при контроле действий системы.

Таблица 131. Значения уровня контроля действий

Возможное значение	Можно указывать в системных значениях QAUDLVL и QAUDLVL2	Можно указывать в команде CHGUSRAUD	Описание
*NONE	Да	Да	Если системное значение QAUDLVL равно *NONE, то в журнале не регистрируются никакие действия на уровне системы. Регистрируются только действия отдельных пользователей в соответствии со значениями AUDLVL в их пользовательских профайлах. Если значение AUDLVL в пользовательском профайле равно *NONE, то никакого дополнительного контроля действий этого пользователя нет. Контролируются те действия этого пользователя, которые указаны в системном значении QAUDLVL.
*ATNEVT	Да	Нет	События, требующие внимания: система заносит в журнал запись в случае события, требующего дальнейшей проверки. Эта информация позволяет определить потенциальную значимость данного события в системе.
*AUTFAIL	Да	Да	Ошибки прав доступа: регистрируются неудачные попытки входа в систему и доступа к объектам. Значение *AUTFAIL может регулярно применяться для выявления пользователей, которые пытаются выполнить в системе несанкционированные действия. Кроме того, *AUTFAIL может применяться при переходе на более высокий уровень защиты и для проверки защиты ресурсов нового приложения.
*CMD	Нет	Да	Команды: система заносит в журнал текст команд, выполняемых пользователем. Если команда запускается из программы на языке CL, которая создана с параметрами LOG(*NO) и ALWRTVSRC(*NO), то регистрируется только имя команды и ее библиотека. Значение *CMD может применяться для получения информации о действиях отдельного пользователя, например системного администратора.
*CREATE	Да	Да	Создание объектов: система заносит в журнал запись при создании нового или замене существующего объекта. Значение *CREATE можно применять для отслеживания создания и повторной компиляции программ.

Таблица 131. Значения уровня контроля действий (продолжение)

Возможное значение	Можно указывать в системных значениях QAUDLVL и QAUDLVL2	Можно указывать в команде CHGUSRAUD	Описание
*DELETE	Да	Да	Удаление объектов: система заносит в журнал запись при удалении объекта.
*JOBBAS	Да	Да	Основные функции задания: в журнале регистрируются действия над заданием, такие как запуск задания и прекращение его выполнения, блокирование, разблокирование, отмена и изменение задания.
*JOBCHGUSR	Да	Да	Изменение пользователя задания: Регистрируются изменения профайла пользователя или группы активной нити.
*JOBDTA	Да	Да	Задачи задания: в журнале регистрируются действия над заданием, такие как запуск задания и прекращение его выполнения, блокирование, разблокирование, отмена и изменение задания, изменения профайла пользователя или группы активной нити. Значение *JOBDTA может применяться для получения информации о пользователях, запускающих пакетные задания. *JOBDTA включает значения *JOBBAS и *JOBCHGUSR, позволяющие точнее настроить контроль.
*NETBAS	Да	Да	Сетевые функции: работа с правилами IP, соединениями через сокеты, фильтром поиска в каталоге APPN и фильтром конечных точек APPN.
*NETCLU	Да	Да	Операции с кластером или с группой ресурсов кластера: в журнал контроля заносится запись, если происходит любое из следующих событий: <ul style="list-style-type: none"> • Добавляется, создается или удаляется узел кластера или группа ресурсов кластера. • Узел кластера или группа ресурсов кластера обновляется, удаляется, запускается или останавливается. • Отказ системы, при котором доступ автоматически переключается на другую систему. • Переключение с одной системы кластера на другую вручную.

Таблица 131. Значения уровня контроля действий (продолжение)

Возможное значение	Можно указывать в системных значениях QAUDLVL и QAUDLVL2	Можно указывать в команде CHGUSRAUD	Описание
*NETCMN	Да	Да	<p>Контроль сетевых соединений: в журнале контроля регистрируются нарушения, обнаруженные программой APPN Filter, если настроен контроль фильтра поиска в каталоге и фильтра конечных точек.</p> <p>Значение *NETCMN состоит из нескольких значений контроля, позволяющих более точно настроить функцию контроля. Они перечислены ниже:</p> <p>*NETBAS *NETCLU *NETFAIL *NETSCK</p>
*NETFAIL	Да	Да	<p>Сбой в сети: в журнал контроля заносится запись при попытке подключиться к несуществующему порту TCP/IP, либо отправить информацию через закрытый или недоступный порт TCP/IP.</p>
*NETSCK	Да	Да	<p>Работа с сокетами: в журнал контроля заносятся записи о следующих событиях:</p> <ul style="list-style-type: none"> • Принят запрос на установление входящего соединения с сокетом TCP/IP. • Установлено исходящее соединение с сокетом TCP/IP. • Протокол DHCP присвоил IP-адрес. • Протоколу DHCP не удалось присвоить IP-адрес, так как нет свободных IP-адресов. • Почтовое сообщение отфильтровано или отклонено.
*OBJMGT	Да	Да	<p>Задачи управления объектом: в журнале сохраняется информация об операциях переименования объекта и его перемещения в другую библиотеку. С помощью значения *OBJMGT можно отслеживать копирование конфиденциальной информации путем перемещения объекта в другую библиотеку.</p>
*OPTICAL	Да	Да	<p>Функции для работы с оптической памятью: контролируются все функции для работы с оптической памятью, включая функции для оптических файлов, оптических каталогов, оптических томов и оптических кассет. С помощью значения *OPTICAL можно отслеживать попытки создания и удаления оптического каталога.</p>
*PGMADP	Да	Да	<p>Принятие прав доступа: система заносит в журнал, когда доступ к объекту предоставляется на основании принятых прав доступа. С помощью значения *PGMADP можно протестировать применение принятых прав доступа в новом приложении.</p>

Таблица 131. Значения уровня контроля действий (продолжение)

	Возможное значение	Можно указывать в системных значениях QAUDLVL и QAUDLVL2	Можно указывать в команде CHGUSRAUD	Описание
I	*PGMFAIL	Да	Да	Сбои в программах: если при выполнении программы происходит нарушение целостности данных, система заносит запись в журнал контроля. Значение *PGMFAIL может применяться при переходе на более высокий уровень защиты и для тестирования нового приложения.
I	*PRTDTA	Да	Да	Функции печати: сохраняется информация о печати буферного файла, печати напрямую из программы и отправке буферного файла на удаленный принтер. С помощью значения *PRTDTA можно отслеживать печать конфиденциальной информации.
	*SAVRST	Да	Да	Операции восстановления: значение *SAVRST позволяет отслеживать попытки восстановления запрещенных объектов.
I	*SECCFG	Да	Да	Конфигурация защиты: в журнал контроля заносятся записи о следующих событиях: <ul style="list-style-type: none"> Создание, изменение или удаление пользовательских профайлов. Изменение программ, системных значений, параметров выполнения подсистемы и атрибутов контроля объекта. Сброс пароля QSECOFR и восстановление пароля, поставляемого IBM. Восстановления пароля по умолчанию для администратора сервисных средств.
I	*SECDIRSRV	Да	Да	Функции службы каталогов: в журнал контроля заносятся записи о следующих событиях: <ul style="list-style-type: none"> Изменение или обновление параметров контроля, прав доступа, паролей или принадлежности объекта. Успешное связывание или аннулирование связывания. Изменения стратегий защиты каталогов (например, стратегии работы с паролями).
I	*SECIPC	Да	Да	Взаимодействие между процессами: в журнал контроля заносятся записи о следующих событиях: <ul style="list-style-type: none"> Изменение принадлежности объекта IPC или прав доступа к нему. Создание, удаление или получение объекта IPC. Подключение общей памяти.

Таблица 131. Значения уровня контроля действий (продолжение)

Возможное значение	Можно указывать в системных значениях QAUDLVL и QAUDLVL2	Можно указывать в команде CHGUSRAUD	Описание
I *SECNAS	Да	Да	<p>Действия службы сетевой идентификации: в журнал контроля заносятся записи о следующих событиях:</p> <ul style="list-style-type: none"> • Служебный паспорт недействителен. • Субъекты служб не совпадают. • Субъекты клиентов не совпадают. • Несовпадение IP-адреса паспорта. • Не удалось расшифровать паспорт. • Не удалось расшифровать идентификационные данные. • Область не входит в локальные области и области клиента. • Паспорт используется повторно. • Срок действия паспорта еще не начался. • Не совпадает удаленный или локальный IP-адрес. • При расшифровке KRB_AP_PRIV или KRB_AP_SAFE обнаружена ошибка в контрольной сумме. • Для KRB_AP_PRIV или KRB_AP_SAFE: ошибка системного времени, ошибка воспроизведения или ошибка порядка следования. • При принятии набора графических символов: одноразовое разрешение с истекшим сроком действия, неправильная контрольная сумма или связывание каналов. • При развертывании или проверке набора графических символов: устаревший контекст, ошибка расшифровки/декодирования, неправильная контрольная сумма или ошибка в порядковом номере.
I *SECRUN	Да	Да	<p>Функции защиты времени выполнения: в журнале контроля сохраняется информация об изменении принадлежности объекта, прав доступа и основной группы.</p>
I *SECCKD	Да	Да	<p>Дескрипторы сокетов: в журнал контроля заносятся записи о следующих событиях:</p> <ul style="list-style-type: none"> • Дескриптор сокета передан другому заданию. • Получен дескриптор сокета. • Дескриптор сокета непригоден для использования.

Таблица 131. Значения уровня контроля действий (продолжение)

Возможное значение	Можно указывать в системных значениях QAUDLVL и QAUDLVL2	Можно указывать в команде CHGUSRAUD	Описание
I *SECVFY	Да	Да	<p>Функции проверки: в журнал контроля заносятся записи о следующих событиях:</p> <ul style="list-style-type: none"> Создана ссылка на профайл или выдано временное разрешение. Все временные маркеры профайла аннулированы. Выдано максимальное число разрешений. Все маркеры профайла пользователя удалены. Идентифицирован пользовательский профайл. Целевой профайл был изменен во время сеанса работы с удаленной системой.
I *SECVLDL	Да	Да	<p>Операции контрольного списка: в журнал контроля заносятся записи о следующих событиях:</p> <ul style="list-style-type: none"> Добавление, изменение, удаление или поиск записи контрольного списка. Успешная или неудачная проверка записи контрольного списка.
*SECURITY	Да	Да	<p>Задачи защиты: регистрируются события, влияющие на защиту, например, изменение пользовательского профайла или системного значения. Значение *SECURITY может применяться для регистрации всех операций с параметрами защиты.</p> <p>Значение *SECURITY состоит из нескольких значений контроля, позволяющих более точно настроить функцию контроля. Эти значения перечислены ниже:</p> <ul style="list-style-type: none"> *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECCKD *SECVFY *SECVLDL
*SERVICE	Да	Да	<p>Задачи обслуживания: в журнале контроля регистрируется применение сервисных средств, таких как DMPOBJ (Создать дампы объекта) и STRCPYSCN (Начать копирование экрана). Значение *SERVICE позволяет отслеживать попытки обхода защиты с помощью сервисных средств.</p>
*SPLFDTA	Да	Да	<p>Операции над буферными файлами: в журнале регистрируются действия, выполняемые над буферными файлами, включая их создание, копирование и отправку. Значение *SPLFDTA позволяет отслеживать попытки печати или отправки конфиденциальных данных.</p>

Таблица 131. Значения уровня контроля действий (продолжение)

Возможное значение	Можно указывать в системных значениях QAUDLVL и QAUDLVL2	Можно указывать в команде CHGUSRAUD	Описание
*SYSMGT	Да	Да	Задачи управления системами: в журнал контроля заносятся записи об операциях управления системами, в том числе об изменении списка ответов или расписания включения и отключения питания. Значения *SYSMGT позволяет отслеживать попытки обхода защиты с помощью функций управления системами.

Записи журнала контроля за действиями:

Этот раздел содержит информацию о записях, которые заносятся в журнал при различных значениях контроля действий, указанных в системных значениях QAUDLVL и QAUDLVL2 и в пользовательском профайле.

Эта информация включает:

- Тип записи журнала QAUDJRN.
- Модельный файл базы данных для вывода, который может применяться для определения записи при создании файла вывода с помощью команды DSPJRN. Форматы записей для модельных файлов базы данных подробно рассматриваются в разделе Приложение F, “Макет записей журнала контроля”, на стр. 593.
- Подробная информация о типе записи. Некоторые типы записей журнала применяются для регистрации нескольких типов событий. Поле подробной информации о типе записи позволяет идентифицировать тип события.
- ИД сообщения, в котором может быть задана особая информация о записи журнала.

Таблица 132. Записи журнала контроля за действиями

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
Контроль действий				
*ATNEVT	IM	QASYIMJ5	P	Обнаружено потенциальное вторжение. Для того чтобы определить, действительно ли это вторжение или же ожидаемое и разрешенное действие, необходима дальнейшая проверка.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
*AUTFAIL	AF	QASYAFJE/J4/J5	A	Предпринята попытка выполнения операции или обращения к объекту при отсутствии необходимых прав доступа.
			B	Запрещенная инструкция
			C	Ошибка проверки
			D	Применение неподдерживаемого интерфейса, ошибка домена объекта
			E	Ошибка аппаратной защиты памяти, выход за границы постоянной памяти программы
			F	Ошибка проверки прав доступа ICAPL.
			G	Ошибка идентификации ICAPL.
			H	Действие программы выхода, выполняющей просмотр.
			I	Запрещено наследование Java для системы
			J	Предпринята попытка внести в расписание или отправить на выполнение задание с описанием, в котором указан пользовательский профайл. При этом пользователь, предпринявший попытку, не имеет прав доступа *USE к этому профайлу.
			K	Предпринята попытка выполнить операцию при отсутствии необходимых специальных прав доступа.
			Нет	Разрешение профайла не является повторно создаваемым.
			O	Нет необходимых прав доступа к объекту оптической памяти
			P	Предпринята попытка использования описателя профайла, недопустимого в API QWTSETP.
			R	Ошибка аппаратной защиты
			S	Попытка выполнить вход в систему по умолчанию.
			T	Нет прав доступа к порту TCP/IP.
			U	Недопустимый запрос прав доступа пользователя.
			V	Кратковременное разрешение не позволяет создать новое разрешение.
			W	Кратковременное разрешение неприменимо для обмена.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
			X	Системное нарушение, см. описание в разделе Записи журнала AF (ошибка прав доступа)
			D	Нет прав доступа к текущему полю JUID при очистке JUID.
			Z	Нет прав доступа к текущему полю JUID при настройке JUID.
	CV	QASYCVJ4/J5	E	Соединение завершено аварийно.
			Ч	Соединение отклонено.
	DI	QASYDIJ4/J5	AF	Недостаточные права доступа.
			PW	Неверный пароль.
	GR	QASYGRJ4/J5	F	Операции по регистрации функции.
	KF	QASYKFJ4/J5	P	Введен неправильный пароль.
	IP	QASYIPJE/J4/J5	F	Недостаточно прав доступа для запроса IPC.
	PW	QASYPWJE/J4/J5	A	Сбой связывания APPC.
			C	Сбой CHKPWD.
			D	Введен неправильный ИД пользователя сервисных средств.
			E	Введен неправильный пароль ИД пользователя сервисных средств.
			P	Введен неправильный пароль.
			Q	Попытка войти в систему (идентификация пользователя) не удалась, поскольку пользовательский профайл отключен.
			Ч	Попытка войти в систему (идентификация пользователя) не удалась, поскольку срок действия пароля истек.
			S	SQL расшифровал недопустимый пароль.
			U	Неверное имя пользователя.
			X	Пользовательский профайл сервисных средств отключен.
			D	Имя пользователя сервисных средств недопустимо.
			Z	Пароль сервисных средств недопустим.
	VC	QASYVCJE/J4/J5	Ч	Соединение отклонено из-за неправильного пароля.
	VO	QASYVOJ4/J5	U	Неудачная проверка записи контрольного списка.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	VN	QASYVNJE/J4/J5	Ч	Вход в сеть запрещен из-за истекшего срока действия учетной записи пользователя, неправильно введенного пароля или ИД пользователя.
	VP	QASYVPJE/J4/J5	P	Использован неправильный сетевой пароль.
	X1	QASYX1J5	F	Идентификационный маркер не передан.
			U	Из идентификационного маркера не получено имя пользователя.
	XD	QASYXDJ5	G	Имена групп (связанные с записью DI)
*CMD ¹	CD	QASYCDJE/J4/J5	C	Команда выполнена.
			L	Использован оператор CL S/36E.
			O	Запущена команда оператора CL S/36E.
			P	Запущена процедура S/36E.
			S	Команда выполнена после замены.
			U	Использована команда утилиты S/36E.
*CREATE ²	CO	QASYCOJE/J4/J5	Нет	Создание нового объекта, кроме создания объекта в библиотеке QTEMP.
			Ч	Замена существующего объекта.
	DI	QASYDIJ4/J5	CO	Объект создан.
	XD	QASYXDJ5	G	Имена групп (связанные с записью DI)
*DELETE ²	DO	QASYDOJE/J4/J5	A	Объект удален.
			C	Выполнена фиксация ожидающего удаления.
			D	Выполнен откат ожидающего создания.
			P	Ожидающее удаление.
			Ч	Выполнен откат ожидающего удаления.
	DI	QASYDIJ4/J5	DO	Объект удален.
	XD	QASYXDJ5	G	Имена групп (связанные с записью DI)
*JOBAS	JS	QASYJSJ5	A	Использование команды ENDJOBABN.
			B	Задание отправлено на выполнение.
			C	Задание изменено.
			E	Задание завершено.
			H	Задание заблокировано.
			I	Задание отсоединено.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
			N	Использование команды ENDJOB.
			P	В предварительное задание добавлен запрос на запуск программы.
			Q	Изменились атрибуты запроса.
			R	Заблокированное задание разблокировано.
			S	Задание запущено.
			U	Команда CHGUSRTRC.
*JOBCHGUSR	JS	QASYJSJ5	M	Изменение профайла пользователя или группы.
			T	Изменение профайла пользователя или группы с помощью одноразового разрешения.
*JOBDTA	JS	QASYJSJE/J4/J5	A	Использование команды ENDJOBABN.
			B	Задание отправлено на выполнение.
			C	Задание изменено.
			E	Задание завершено.
			H	Задание заблокировано.
			I	Задание отсоединено.
			M	Изменение профайла пользователя или группы.
			Нет	Использование команды ENDJOB.
			P	В предварительное задание добавлен запрос на запуск программы.
			Q	Изменились атрибуты запроса.
			Ч	Задание разблокировано.
			S	Задание запущено.
			T	Изменение профайла пользователя или группы с помощью одноразового разрешения.
			U	Команда CHGUSRTRC.
	SG	QASYSGJE/J4/J5	A	Асинхронная обработка сигналов i5/OS.
			P	Асинхронная обработка сигнала PASE.
	VC	QASYVCJE/J4/J5	S	Соединение запущено.
			E	Соединение завершено.
	VN	QASYVNJE/J4/J5	F	Получен запрос на выход из системы.
			O	Получен запрос на вход в систему.
	VS	QASYVSJE/J4/J5	S	Начат сеанс сервера.
			E	Завершен сеанс сервера.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
*NETBAS	CV	QASYCVJE/J4/J5	C	Соединение установлено.
			E	Соединение завершено нормально
			Ч	Соединение отклонено.
	IR	QASYIRJ4/J5	L	Правила IP загружены из файла.
			Нет	Выгружены правила IP для соединения с защитой IP.
			P	Загружены правила IP для соединения с защитой IP.
			Ч	Правила IP прочитаны и скопированы в файл.
			U	Правила IP выгружены (удалены).
			1	1-й этап согласования.
			2	2-й этап согласования.
	ND	QASYNDJE/J4/J5	A	При проверке фильтра поиска в каталоге с помощью программы поддержки фильтров APPN обнаружено нарушение.
			A	При проверке фильтра конечных точек с помощью программы поддержки фильтров APPN обнаружено нарушение.
*NETCLU	CU	QASYCUJE/J4/J5	M	Создание объекта с помощью операций управления кластерами.
			Ч	Создание объекта с помощью средств управления группой ресурсов кластера (*GRP).
*NETCMN	CU	QASYCUJE/J4/J5	M	Создание объекта с помощью операций управления кластерами.
			Ч	Создание объекта с помощью средств управления группой ресурсов кластера (*GRP).
	CV	QASYCVJ4/J5	C	Соединение установлено.
			E	Соединение завершено нормально
			L	Правила IP загружены из файла.
	IR	QASYIRJ4/J5	Нет	Выгружено правило IP для соединения с защитой IP.
			P	Загружены правила IP для соединения с защитой IP.
			Ч	Правила IP прочитаны и скопированы в файл.
			U	Правила IP выгружены (удалены).
			1	1-й этап согласования.
			2	2-й этап согласования.
				IS

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	ND	QASYNDJE/J4/J5	A	При проверке фильтра поиска в каталоге с помощью программы поддержки фильтров APPN обнаружено нарушение.
	NE	QASYNEJE/J4/J5	A	При проверке фильтра конечных точек с помощью программы поддержки фильтров APPN обнаружено нарушение.
	SK	QASYSKJ4/J5	A	Принято
			C	Соединение
			D	Присвоен адрес DHCP
			F	Фильтрованная почта
			P	Порт недоступен
			Ч	Почта отклонена
			U	Адрес DHCP не присвоен
*NETFAIL	SK	QASYSKJ4/J5	P	Порт недоступен
*NETSCK	SK	QASYSKJ4/J5	A	Принято
			C	Соединение
			D	Присвоен адрес DHCP
			F	Фильтрованная почта
			Ч	Почта отклонена
			U	Адрес DHCP не присвоен
*OBJMGT ²	DI	QASYDIJ4/J5	OM	Переименование объекта
	OM	QASYOMJE/J4/J5	M	Перемещение объекта в другую библиотеку.
			Ч	Изменение имени объекта.
*OFCSRVR	ML	QASYMLJE/J4/J5	O	Открытие почтового протокола.
	SD	QASYSDJE/J4/J5	S	Изменение системного каталога рассылки.
*OPTICAL	O1	QASYO1JE/J4/J5	Ч	Открытие файла или каталога.
			U	Получить или изменить атрибуты
			D	Удаление каталога
			C	Создать каталог
			X	Заблокированный оптический файл разблокирован
	O2	QASYO2JE/J4/J5	C	Копирование файла или каталога.
			Ч	Переименование файла
			B	Создание резервной копии файла или каталога.
			S	Сохранение заблокированного оптического файла
			M	Перемещение файла

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	O3	QASY03JE/J4/J5	I	Инициализация тома
			B	Резервный том.
			Нет	Переименование тома
			C	Преобразовать резервный том в основной
			M	Импорт
			E	Экспорт
			L	Изменение списка прав доступа
			A	Изменение атрибутов тома
			Ч	Абсолютное чтение
*PGMADP	AP	QASYAPJE/J4/J5	S	Запущена программа, принимающая права доступа. Запись создается в момент первого использования принятых прав доступа для доступа к объекту, а не в момент помещения программы в стек вызовов.
			E	Завершена работа программы, принимающей права доступа. Запись создается в момент удаления программы из стека вызовов. Если одна и та же программа присутствует в стеке вызовов несколько раз, то запись о ее окончании будет добавлена, когда последняя копия программы будет удалена из стека.
			A	При активации программы были использованы принятые права доступа.
*PGMFAIL	AF	QASYAFJE/J4/J5	B	Запущена программа, использующая команды машинного интерфейса с ограниченным доступом.
			C	Восстановлена программа, не прошедшая проверку при восстановлении. Информация о сбое, произошедшем при проверке содержится в поле <i>Тип нарушения контрольного значения</i> .
			D	Программа обратилась к объекту с помощью неподдерживаемого интерфейса или вызываемой программы, не указанной в списке вызываемых API.
			E	Нарушение аппаратной защиты памяти.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
			Ч	Предпринята попытка обновления объекта, предназначенного только для чтения. (Ведение протокола расширенной аппаратной защиты памяти ведется только на уровне безопасности 40 и выше).
*PRTDTA	PO	QASYPOJE/J4/J5	D	Вывод принтера напечатан непосредственно на принтер.
			Ч	Вывод был отправлен для печати в удаленную систему.
			S	Вывод принтера помещен в буфер и распечатан.
*SAVRST ²	OR	QASYORJE/J4/J5	Нет	В системе восстановлен новый объект.
			E	В системе восстановлен объект, заместивший уже существующий.
	RA	QASYRAJE/J4/J5	A	Права доступа к восстановленному объекту изменены системой. ³
	RJ	QASYRJJE/J4/J5	A	Восстановлено описание задания, содержащее имя профайла.
	RO	QASYROJE/J4/J5	A	Владелец восстановленного объекта изменен на QDFTOWN. ³
	RP	QASYRPJE/J4/J5	A	Восстановлена программа, принимающая права доступа владельца.
	RQ	QASYRQJE/J4/J5	A	Восстановлен объект *CRQD с параметром PROFILE(*OWNER).
	RU	QASYRUJE/J4/J5	A	Права доступа пользовательского профайла восстановлены с помощью команды RSTAUT.
	RZ	QASYRZJE/J4/J5	A	Основная группа восстановленного объекта была изменена.
			O	Контроль объекта изменен с помощью команды CHGOBJAUD.
			U	Контроль пользователя изменен с помощью команды CHGUSRAUD.
*SECCFG	AD	QASYADJE/J4/J5	D	Контроль DLO (объекта библиотеки документов) изменен с помощью команды CHGDLOAUD.
			O	Контроль объекта изменен с помощью команды CHGOBJAUD или CHGAUD.
			S	Атрибут просмотра был изменен с помощью команды CHGATR или API Qp0lSetAttr, либо при создании объекта.
			U	Контроль пользователя изменен с помощью команды CHGUSRAUD.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	AU	QASYAUJ5	E	Изменение конфигурации EIM.
	CP	QASYCPJE/J4/J5	A	Создание, изменение или восстановление пользовательского профайла при использовании QSYSRESPA API.
	CQ	QASYCQJE/J4/J5	A	Изменение объекта *CRQD.
	CY	QASYCYJ4/J5	A	Функция управления доступом
			F	Функции управления средствами
			M	Функции главного ключа
	DO	QASYDOJE/J4/J5	A	Объект был удален вне режима управления фиксацией.
			C	Зафиксированное ожидающее удаление объекта.
			D	Отменено ожидающее создание объекта.
			P	Ожидающее удаление объекта (удаление выполнено в режиме управления фиксацией)
			Ч	Отменено ожидающее удаление объекта.
	DS	QASYDSJE/J4/J5	A	Запрошен сброс пароля DST QSECOFR на определенный системой пароль по умолчанию.
			C	Изменен профайл DST.
	EV	QASYEVJ4/J5	A	Добавление.
			C	Изменение.
			D	Удаление.
			I	Инициализация пространства переменных среды.
	GR	QASYGRJ4/J5	A	Добавлена программа выхода
			D	Удалена программа выхода
			F	Действие по регистрации функции
			Ч	Замещена программа выхода
	JD	QASYJDJE/J4/J5	A	Изменен параметр USER описания задания.
	KF	QASYKFJ4/J5	C	Операция с сертификатом.
			K	Работа с файлом связки ключей.
			T	Работа с надежным базовым сертификатом.
	NA	QASYNAJE/J4/J5	A	Изменены сетевые атрибуты.
	PA	QASYPAJE/J4/J5	A	Программа настроена на прием прав доступа владельца.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	SE	QASYSEJE/J4/J5	A	Изменение записи маршрутизации подсистемы.
	SO	QASYSOJ4/J5	A	Добавление записи.
			C	Изменение записи.
			Ч	Удаление записи.
	SV	QASYSVJE/J4/J5	A	Системное значение изменено.
			B	Изменены атрибуты обслуживания.
			C	Изменение системного времени.
			E	Изменение опции
			F	Изменение атрибута системного журнала
	VA	QASYVAJE/J4/J5	S	Список управления доступом успешно изменен.
			F	Неудачная попытка изменения списка управления доступом.
			V	Успешная проверка записи контрольного списка.
	VU	QASYVUJE/J4/J5	G	Запись группы изменена.
			M	Изменена глобальная информация пользовательского профайла.
			U	Изменена запись пользователя.
*SECDIRSRV	DI	QASYDIJE/J4/J5	AD	Изменение контроля.
			BN	Успешное связывание
			CA	Изменение прав доступа
			CP	Изменение пароля
			OW	Изменение принадлежности
			PO	Изменение стратегии
			UB	Связывание успешно аннулировано
*SECIPC	IP	QASYIPJE/J4/J5	A	Изменены права доступа к объекту IPC или его владлец.
			C	Создание объекта IPC.
			D	Удаление объекта IPC.
			G	Получение объекта IPC.
*SECNAS	X0	QASYX0J4/J5	1	Служебный паспорт действителен.
			2	Субъекты служб не совпадают.
			3	Субъекты клиентов не совпадают.
			4	Несовпадение IP-адреса паспорта.
			5	Не удалось расшифровать паспорт.
			6	Не удалось расшифровать удостоверение.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
			7	Область находится за пределами локальной области и области клиента.
			8	Попытка использования паспорта для имитации.
			9	Паспорт еще не действителен.
			A	Ошибка при расшифровке контрольной суммы KRB_AP_PRIV или KRB_AP_SAFE
			B	Несовпадение IP-адреса удаленной системы
			C	Несовпадение IP-адреса локальной системы
			D	Ошибка метки времени KRB_AP_PRIV или KRB_AP_SAFE
			E	Ошибка повторного использования KRB_AP_PRIV или KRB_AP_SAFE
			F	Ошибка в порядке следования KRB_AP_PRIV KRB_AP_SAFE
			K	Запуск GSS - истек срок действия временного разрешения
			L	Запуск GSS - ошибка в контрольной сумме
			M	Запуск GSS - связывания канала
			Нет	Развертывание GSS или проверка с помощью GSS, информация с истекшим сроком действия.
			O	Развертывание GSS или проверка с помощью GSS, расшифровка.
			P	Развертывание GSS или проверка с помощью GSS, ошибка в контрольной сумме.
			Q	Развертывание GSS или проверка с помощью GSS, ошибка в последовательности.
*SECRUN	CA	QASYCAJE/J4/J5	A	Изменения списка прав доступа или прав доступа к объекту.
	OW	QASYOWJE/J4/J5	A	Изменение принадлежности объекта.
	PG	QASYPGJE/J4/J5	A	Изменение основной группы объекта.
*SECCKD	GS	QASYGSJE/J4/J5	G	Дескриптор сокета присвоен другому заданию. (Запись журнала контроля GS создается только в том случае, если для текущего задания запись не создана).
			Ч	Получение дескриптора.
			U	Невозможно воспользоваться дескриптором.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
*SECURITY	AD	QASYADJE/J4/J5	D	Контроль DLO (объекта библиотеки документов) изменен с помощью команды CHGDLOAUD.
			O	Контроль объекта изменен с помощью команды CHGOBJAUD или CHGAUD.
			S	Изменение атрибута просмотра командой CHGATR или API Qp01SetAttr.
			U	Контроль пользователя изменен с помощью команды CHGUSRAUD.
	XI	QASYADJE/J4/J5	D	Успешная передача опознавательного маркера
			G	Успешное получение данных о пользователе из опознавательного маркера
	AU	QASYAUJ5	E	Изменение конфигурации EIM.
	CA	QASYCAJE/J4/J5	A	Изменения списка прав доступа или прав доступа к объекту.
	CP	QASYCPJE/J4/J5	A	Создание, изменение или восстановление пользовательского профайла при использовании API QSYRESPA.
	CQ	QASYCQJE/J4/J5	A	Изменение объекта *CRQD.
	CV	QASYCVJ4/J5	C	Соединение установлено.
			E	Соединение завершено нормально
			Ч	Соединение отклонено.
	CY	QASYCYJ4/J5	A	Функция управления доступом
			F	Функции управления средствами
			M	Функции главного ключа
	DI	QASYDIJ4/J5	AD	Изменение контроля
			BN	Успешное связывание
			CA	Изменение прав доступа
			CP	Изменение пароля
			OW	Изменение принадлежности
			PO	Изменение стратегии
			UB	Связывание успешно аннулировано
	DO	QASYDOJE/J4/J5	A	Объект был удален вне режима управления фиксацией.
			C	Зафиксированное ожидающее удаление объекта.
			D	Отменено ожидающее создание объекта.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
			P	Ожидающее удаление объекта (удаление выполнено в режиме управления фиксацией)
			Ч	Отменено ожидающее удаление объекта.
	DS	QASYDSJE/J4/J5	A	Запрошен сброс пароля DST QSECOFR на определенный системой пароль по умолчанию.
			C	Изменен профайл DST.
	EV	QASYEVJ4/J5	A	Добавление.
			C	Изменение.
			D	Удаление.
			I	Инициализация пространства переменных среды.
	GR	QASYGRJ4/J5	A	Добавлена программа выхода
			D	Удалена программа выхода
			F	Действие по регистрации функции
			Ч	Замещена программа выхода
	GS	QASYGSJE/J4/J5	G	Дескриптор сокета присвоен другому заданию. (Запись журнала контроля GS создается только в том случае, если для текущего задания запись не создана).
			Ч	Получение дескриптора.
			U	Невозможно воспользоваться дескриптором.
	IP	QASYIPJE/J4/J5	A	Изменены права доступа к объекту IPC или его владелец.
			C	Создание объекта IPC.
			D	Удаление объекта IPC.
			G	Получение объекта IPC.
	JD	QASYJDJE/J4/J5	A	Изменен параметр USER описания задания.
	KF	QASYKFJ4/J5	C	Операция с сертификатом.
			K	Работа с файлом связки ключей.
			T	Работа с надежным базовым сертификатом.
	NA	QASYNAJE/J4/J5	A	Изменены сетевые атрибуты.
	OW	QASYOWJE/J4/J5	A	Изменение принадлежности объекта.
	PA	QASYPAJE/J4/J5	A	Программа настроена на прием прав доступа владельца.
	PG	QASYPGJE/J4/J5	A	Изменение основной группы объекта.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	PS	QASYPSJE/J4/J5	A	Целевой пользовательский профайл изменен во время сеанса удаленного доступа.
			E	Пользователь Office завершил работу от имени другого пользователя.
			H	Была создан описатель профайла с использованием API QSYGETPH.
			I	Все временные маркеры профайла аннулированы.
			M	Выдано максимальное число разрешений.
			P	Для пользователя создан маркер профайла.
			Ч	Все маркеры профайла пользователя удалены.
			S	Пользователь Office начал работу от имени другого пользователя.
			V	Пользовательский профайл идентифицирован.
	SE	QASYSEJE/J4/J5	A	Изменение записи маршрутизации подсистемы.
	SO	QASYSOJ4/J5	A	Добавление записи.
			C	Изменение записи.
			Ч	Удаление записи.
	SV	QASYSVJE/J4/J5	A	Системное значение изменено.
			B	Изменены атрибуты обслуживания.
			C	Изменение системного времени.
			E	Изменение опции
			F	Изменение атрибута системного журнала
	VA	QASYVAJE/J4/J5	S	Список управления доступом успешно изменен.
			F	Неудачная попытка изменения списка управления доступом.
	VO		V	Удачная проверка записи контрольного списка.
	VU	QASYVUJE/J4/J5	G	Запись группы изменена.
			M	Изменена глобальная информация пользовательского профайла.
			U	Изменена запись пользователя.
	X0	QASYX0J4/J5	1	Служебный паспорт действителен.
			2	Субъекты служб не совпадают.
			3	Субъекты клиентов не совпадают.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
			4	Несовпадение IP-адреса паспорта.
			5	Не удалось расшифровать паспорт.
			6	Не удалось расшифровать удостоверение.
			7	Область находится за пределами локальной области и области клиента.
			8	Попытка использования паспорта для имитации.
			9	Паспорт еще не действителен.
			A	Ошибка при расшифровке контрольной суммы KRB_AP_PRIV или KRB_AP_SAFE
			B	Несовпадение IP-адреса удаленной системы
			C	Несовпадение IP-адреса локальной системы
			D	Ошибка метки времени KRB_AP_PRIV или KRB_AP_SAFE
			E	Ошибка повторного использования KRB_AP_PRIV или KRB_AP_SAFE
			F	Ошибка в порядке следования KRB_AP_PRIV KRB_AP_SAFE
			K	Запуск GSS - истек срок действия временного разрешения
			L	Запуск GSS - ошибка в контрольной сумме
			M	Запуск GSS - связывания канала
			Нет	Развертывание GSS или проверка с помощью GSS, информация с истекшим сроком действия.
			O	Развертывание GSS или проверка с помощью GSS, расшифровка.
			P	Развертывание GSS или проверка с помощью GSS, ошибка в контрольной сумме.
			Q	Развертывание GSS или проверка с помощью GSS, ошибка в последовательности.
*SECVFY	PS	QASYPSJE/J4/J5	A	Целевой пользовательский профайл изменен во время сеанса удаленного доступа.
	X1	QASYX1J5	D	Успешная передача опознавательного маркера
			G	Успешное получение данных о пользователе из опознавательного маркера

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
			E	Пользователь Office завершил работу от имени другого пользователя.
			H	Была создан описатель профайла с использованием API QSYGETPH.
			I	Все временные маркеры профайла аннулированы.
			M	Выдано максимальное число разрешений.
			P	Для пользователя создан маркер профайла.
			Ч	Все маркеры профайла пользователя удалены.
			S	Пользователь Office начал работу от имени другого пользователя.
			V	Пользовательский профайл идентифицирован.
*SECVLDL	VO		V	Успешная проверка записи контрольного списка.
*SERVICE	ST	QASYSTJE/J4/J5	A	Использование сервисного средства.
	VV	QASYVVJE/J4/J5	C	Изменение состояния обслуживания.
			E	Сервер остановлен.
			P	Сервер приостановлен.
			Ч	Сервер перезапущен.
			S	Сервер запущен.
*SPLFDA	SF	QASYSFJE/J4/J5	A	Буферный файл прочитан кем-то, кроме его владельца.
			C	Буферный файл создан.
			D	Буферный файл удален.
			H	Буферный файл заблокирован.
			I	Внутренний файл создан.
			Ч	Буферный файл разблокирован.
			S	Буферный файл сохранен.
			T	Буферный файл восстановлен.
			U	Буферный файл изменен.
			V	Изменились только атрибуты буферного файла, не связанные с защитой.
*SYSMGT	DI	QASYDIJ4/J5	CF	Изменение конфигурации.
			CI	Создание экземпляра
			DI	Удаление экземпляра
			RM	Управление копированием.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	SM	QASYSMJE/J4/J5	B	Опции резервного копирования изменены с помощью xxxxxxxxxx.
			C	Опции автоматической очистки изменены с помощью xxxxxxxxxx.
			D	Изменен объект DRDA*.
			F	Изменена файловая система HFS.
			Net	Выполнена обработка сетевого файла.
			O	Список резервного копирования изменен с помощью xxxxxxxxxx.
			P	Расписание включения и отключения питания изменено с помощью xxxxxxxxxx.
			S	Изменен системный список ответов на сообщения.
			T	Изменены времена восстановления путей доступа.
	VL	QASYVLJE/J4/J5	A	Истек срок действия учетной записи.
			D	Учетная запись отключена.
			L	Истекло время пребывания в системе.
			U	Неизвестно или недоступно.
			W	Рабочая станция недопустима.
Контроль объектов:				
*CHANGE	DI	QASYDIJ4/J5	IM	Импорт каталога LDAP
			ZC	Изменение объекта
	ZC	QASYZCJ4/J5	C	Изменения объекта
			U	Расширение открытого доступа к объекту
	AD	QASYADJEJ4/J5	D	Контроль объекта изменен с помощью команды CHGOBJAUD.
			O	Контроль объекта изменен с помощью команды CHGOBJAUD.
			S	Изменение атрибута просмотра командой CHGATR или API Qp01SetAttr.
			U	Контроль пользователя изменен с помощью команды CHGUSRAUD.
	AU	QASYAUJ5	E	Изменение конфигурации EIM.
	CA	QASYCAJE/J4/J5	A	Изменения списка прав доступа или прав доступа к объекту.
	OM	QASYOMJE/J4/J5	M	Перемещение объекта в другую библиотеку.
			Ч	Изменение имени объекта.

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	OR	QASYORJE/J4/J5	Нет	В системе восстановлен новый объект.
			E	В системе восстановлен объект, заместивший уже существующий.
	OW	QASYOWJE/J4/J5	A	Изменение принадлежности объекта.
	PG	QASYPGJE/J4/J5	A	Изменение основной группы объекта.
	RA	QASYRAJE/J4/J5	A	Права доступа к восстановленному объекту изменены системой.
	RO	QASYROJE/J4/J5	A	Владелец восстановленного объекта изменен на QDFTOWN.
	RZ	QASYRZJE/J4/J5	A	Основная группа восстановленного объекта была изменена.
	GR	QASYGRJ4/J5	F	Операции регистрации функций ⁵
	LD	QASYLDJE/J4/J5	L	Подключение каталога.
			U	Отключение каталога.
	VF	QASYVFJE/J4/J5	A	Файл закрыт из-за административного отключения связи.
			Нет	Файл закрыт из-за нормального отключения связи клиентом.
			S	Файл закрыт из-за завершения сеанса связи.
	VO	QASYVOJ4/J5	A	Добавление записи контрольного списка.
			C	Изменение записи контрольного списка.
			F	Поиск записи контрольного списка.
			Ч	Удаление записи контрольного списка.
	VR	QASYVRJE/J4/J5	F	Неудачная попытка доступа к ресурсам.
			S	Успешный доступ к ресурсам.
	YC	QASYYCJE/J4/J5	C	Изменен объект библиотек документов (DLO).
	ZC	QASYZCJE/J4/J5	C	Изменен объект.
			U	Расширение открытого доступа к объекту.
*ALL ⁴	CD	QASYCDJ4/J5	C	Выполнение команды
	DI	QASYDIJ4/J5	EX	Экспорт каталога LDAP
			ZR	Чтение объекта
	GR	QASYGRJ4/J5	F	Операции регистрации функций ⁵
	LD	QASYLDJE/J4/J5	K	Поиск каталога.
	YR	QASYRJE/J4/J5	Ч	Чтение объекта библиотеки документов (DLO).

I

Таблица 132. Записи журнала контроля за действиями (продолжение)

Значение уровня контроля действий или объектов	Тип записи журнала	Модельный файл вывода базы данных	Подробная запись	Описание
	ZR	QASYZRJE/J4/J5	Ч	Чтение объекта.
1	Это значение можно указать только в параметре AUDLVL пользовательского профайла. Его нельзя использовать в качестве системного значения.			
2	Если контроль над объектом активизирован, то при выполнении операций создания или удаления объекта, а также операций управления объектом и при его восстановлении будут создаваться записи журнала контроля, даже когда эти действия не указаны в уровне контроля.			
3	Информация о возможных изменениях прав доступа при восстановлении объектов приведена в разделе "Восстановление объектов" на стр. 263.			
4	Если выбрано значение *ALL, то записи будут создаваться и для *CHANGE, и для *ALL.			
5	Если объект QUSRSYS/QUSEXRGOBJ *EXITRG находится под контролем.			

Планирование контроля доступа к объектам

Операционная система i5/OS предоставляет возможность сохранять в журнале контроля за действиями информацию о доступе к объекту. Для этого используются системные значения и значения контроля за за объектом для пользователей и объектов. Это называется *контролем за объектом*.

Для контроля за объектом применяется системное значение QAUDCTL, параметр OBJAUD объекта и параметр OBJAUD из пользовательского профайла. Значение OBJAUD для объекта в сочетании со значением OBJAUD для пользователя, работающего с объектом, определяют, какие типы доступа должны регистрироваться в журнале. Системное значение QAUDCTL служит для включения и выключения функции контроля за объектами.

В Табл. 133 показано, каким образом действуют различные сочетания значений OBJAUD для объекта и для пользовательского профайла.

Таблица 133. Как применяются контроль за объектом и контроль за пользователями

Значение OBJAUD для объекта	Значение OBJAUD для пользователя		
	*NONE	*CHANGE	*ALL
*NONE	Нет	Нет	Нет
*USRPRF	Нет	Изменение	Изменение и использование
*CHANGE	Изменение	Изменение	Изменение
*ALL	Изменение и использование	Изменение и использование	Изменение и использование

Контроль за объектом позволяет отслеживать доступ всех пользователей к важному объекту в системе. Кроме того, можно отслеживать доступ к объектам конкретного пользователя. Контроль за объектом предоставляет широкие возможности для отслеживания доступа к наиболее важным объектам в вашей системе.

Эффективный контроль за объектами невозможен без тщательного планирования. При плохо спланированном контроле в журнал заносится слишком много записей - гораздо больше, чем вы сможете проанализировать. При этом может сильно снизиться производительность системы. Например, если присвоить параметру OBJAUD библиотеки значение *ALL, то при каждом обращении системы к библиотеке для поиска объекта будет заноситься запись в журнал контроля. Если эта библиотека часто используется, то в журнал контроля будет поступать огромное число записей.

Ниже приведено несколько примеров применения контроля за объектом.

- Если в вашей организации используются файлы, содержащие важную информацию, то с помощью несложной процедуры вы можете отследить, кто к ним обращается:
 1. С помощью команды Изменить контроль объекта задайте для файла параметр OBJAUD, равный *USRPRF:

```

                          Изменить контроль объекта (CHGOBJAUD)

Введите опции, нажмите Enter.

Объект . . . . . файл
Библиотека . . . . . библиотека
Тип объекта . . . . . *FILE
ASP . . . . . *
Значение контроля объекта . . . . *USRPRF

```

2. С помощью команды CHGUSRAUD установите для каждого пользователя значение OBJAUD, равное *CHANGE или *ALL.
 3. Убедитесь, что системное значение QAUDCTL содержит *OBJAUD.
 4. По истечении некоторого периода времени, достаточного для получения представительной выборки, установите значение OBJAUD в пользовательском профайле равным *NONE или удалите *OBJAUD из системного значения QAUDCTL.
 5. Проанализируйте записи журнала контроля, используя для этого приемы, описанные в разделе “Анализ записей журнала контроля с помощью утилиты запроса или программы” на стр. 315.
- Если вас интересует, кто работает с конкретным файлом, вы можете собрать информацию о всех обращениях к этому файлу за некоторый период времени:
 1. Задайте значения контроля объекта для этого файла независимо от значений для пользовательских профайлов:


```

CHGOBJAUD OBJECT(имя-библиотеки/имя-файла)
                   OBJTYPE(*FILE) OBJAUD(*CHANGE или *ALL)
          
```
 2. Убедитесь, что системное значение QAUDCTL содержит *OBJAUD.
 3. По истечении некоторого промежутка времени, достаточного для получения представительной выборки, установите для параметра объекта OBJAUD значение *NONE.
 4. Проанализируйте записи журнала контроля, используя для этого приемы, описанные в разделе “Анализ записей журнала контроля с помощью утилиты запроса или программы” на стр. 315.
 - Для того чтобы настроить контроль доступа ко всем объектам для определенного пользователя, выполните следующие действия:
 1. С помощью команд CHGOBJAUD и CHGAUD установите значение OBJAUD, равное *USRPRF, для всех объектов:

```

                          Изменить контроль объекта (CHGOBJAUD)

Введите опции, нажмите Enter.

Объект . . . . . *ALL
Библиотека . . . . . *ALLAVL
Тип объекта . . . . . *ALL
ASP . . . . . *
Значение уровня контроля объектов . . . . *USRPRF

```

Внимание: Продолжительность выполнения этой команды зависит от количества объектов в вашей системе и может достигать нескольких часов. Обычно не требуется устанавливать контроль за всеми объектами в системе, так как при этом сильно снижается производительность. Контроль рекомендуется включать для ограниченного набора типов объектов и библиотек.

2. С помощью команды CHGUSRAUD установите для отдельного пользовательского профайла значение OBJAUD, равное *CHANGE или *ALL.
3. Убедитесь, что системное значение QAUDCTL содержит *OBJAUD.
4. После того как будет собран достаточный объем статистики, установите для параметра OBJAUD в пользовательском профайле значение *NONE.

Ссылки, связанные с данной

“Контроль объекта” на стр. 117

Значение контроля за объектом, указанное в пользовательском профайле, используется совместно со значением контроля за объектом, указанным для объекта, для определения необходимости контроля за пользователем, работающим с этим объектом.

Показ контроля объектов:

Команда DSPOBJD показывает информацию о текущем уровне контроля за объектом. Команда DSPDLOAD показывает информацию о текущем уровне контроля за объектом библиотеки документов.

Настройка параметров контроля по умолчанию для объекта:

Параметры контроля для вновь создаваемых объектов можно настроить с помощью системного значения QCRTOBJAUD и параметра CRTOBJAUD библиотек и каталогов.

Например, если вы хотите установить для всех новых объектов в библиотеке INVLIB значение контроля, равное *USRPRF, то введите следующую команду:

```
CHGLIB LIB(INVLIB) CRTOBJAUD(*USRPRF)
```

Эта команда изменяет значение контроля только для новых объектов. Она не влияет на значения контроля объектов, уже существующих в библиотеке.

Следует соблюдать осторожность при использовании значений контроля по умолчанию. Неправильная настройка этих значений может привести к появлению в журнале контроля большого количества ненужных записей. Для того чтобы контроль за объектами в системе работал эффективно, его необходимо тщательно спланировать.

Предотвращение потерь данных контроля

Действия системы в случае, когда в результате сбоя могут быть утеряны записи журнала контроля, определяются двумя системными значениями.

Уровень выгрузки записей контроля

Системное значение QAUDFRCLVL определяет, как часто записи журнала контроля выгружаются из оперативной памяти во вспомогательную память.

Системное значение QAUDFRCLVL работает так же, как аналогичное значение для файлов базы данных. При настройке системного значения QAUDFRCLVL необходимо следовать аналогичным рекомендациям.

Если вы разрешите системе определять, когда следует выгружать записи во вспомогательную память, то она будет стараться выгружать записи в периоды минимальной загруженности системы, вместе с тем не откладывая операцию на слишком долгое время, чтобы появился риск потери данных из-за сбоя подачи питания. Значение по умолчанию: *SYS.

Если вы укажете слишком маленький уровень выгрузки записей, то риск потери данных контроля будет минимальным, однако производительность системы может снизиться. Если в вашем случае недопустимо, чтобы при сбое подачи питания были утеряны какие-либо записи контроля, то установите значение QAUDFRCLVL, равное 1.

Действие при сбое контроля

Системное значение Действие при сбое контроля (QAUDENDACN) определяет, что должна делать система, если ей не удастся занести запись в журнал контроля.

Значение по умолчанию равно *NOTIFY. Если системе не удастся занести запись в журнал контроля, а системное значение QAUDENDACN равно *NOTIFY, то выполняются следующие действия:

1. Системное значение QAUDCTL устанавливается равным *NONE, чтобы предотвратить повторные попытки занесения записей в журнал.
2. В очередь сообщений QSYSOPR и QSYSMSG (если она существует) с интервалом в один час отправляются сообщения CPI2283, до тех пор, пока не будет успешно перезапущена функция контроля.
3. Продолжается обычная работа.
4. Если в системе выполняется IPL, то во время IPL в очередь сообщений QSYSOPR и QSYSMSG отправляется сообщение CPI2284.

Примечание: В большинстве случаев выполнение IPL приводит к устранению неполадки, вызвавшей сбой контроля. После перезапуска системы установите правильное значение для QAUDCTL. Всякий раз при изменении этого системного значения система делает попытку занести запись в журнал контроля.

Для QAUDENDACN можно установить значение *PWRDWNSYS, чтобы при сбое контроля система выключалась. Используйте это значение только в том случае, если система не должна работать при отсутствии контроля. Если системе не удастся занести запись в журнал контроля и системное значение QAUDENDACN равно *PWRDWNSYS, происходит следующее:

1. Система немедленно выключается (так же как и при вводе команды PWRDWNSYS *IMMED).
2. На индикаторе панели управления появляется код B900 3D10.

После этого вы должны выполнить следующие действия:

1. Запустите IPL с системного блока. Проверьте, включено ли устройство, указанное в системном значении консоли (QCONSOLE).
2. Для выполнения IPL пользователь со специальными правами доступа *ALLOBJ и *AUDIT должен войти в систему с консоли.

Система запускается в состоянии с ограничениями; при этом выдается сообщение, указывающее, что останов системы произошел из-за сбоя контроля.

3. Системное значение QAUDCTL устанавливается равным *NONE.
4. Для того чтобы восстановить нормальный режим работы системы, установите системное значение QAUDCTL, отличное от *NONE. При изменении системного значения QAUDCTL система попытается занести запись в журнал контроля. Если ей удастся это сделать, то она переходит в нормальный режим работы.

Если в системе не удалось восстановить нормальный режим работы, то просмотрите протоколы заданий, чтобы определить причину сбоя контроля. Устраните неполадку и сбросьте значение QAUDCTL.

Выключение контроля объектов QTEMP

Выключить контроль объектов QTEMP позволяет значение *NOQTEMP.

В системном значении QAUDCTL можно указать значение *NOQTEMP. Вместе с ним необходимо задать значение *OBJAUD или *AUDLVL. Если функция контроля активна и указано значение *NOQTEMP, то в библиотеке QTEMP не контролируется выполнение следующих действий:

- Изменение и чтение объектов в QTEMP (типы записей журнала ZC, ZR).
- Изменение прав доступа, владельца или основной группы объектов в QTEMP (типы записей журнала CA, OW, PG).

Настройка контроля за действиями с помощью CHGSECAUD

Описание:

С помощью команды CHGSECAUD можно запустить системный контроль за действиями. Для этого нужно убедиться, что журнал защиты существует, и присвоить системному значению QAUDCTL значение *AUDLVL, а системному значению QAUDLVL - набор значений по умолчанию. Набор по умолчанию предусматривает контроль за действиями *AUTFAIL, *CREATE, *DELETE, *SECURITY и *SAVRST.
CHGSECAUD QAUDCTL(*AUDLVL) QAUDLVL(*DFTSET)

Задача:

Настройка системы для регистрации событий, влияющих на защиту, в журнале QAUDJRN.

Средства для ее решения:

CHGSECAUD
DSPSECAUD

Права доступа:

У пользователя должны быть специальные права доступа *ALLOBJ и *AUDIT.

Запись в журнале:

CO (создание объекта)
SV (изменение системного значения)
AD (изменение параметров контроля за объектами и пользователями)

Прим.: Если журнал и получатель журнала не существуют, команда CHGSECAUD создает их. Затем команда CHGSECAUD устанавливается системные значения QAUDCTL, QAUDLVL и QAUDLVL2.

Ссылки, связанные с данной

“Опции меню Инструменты защиты” на стр. 749

Меню Инструменты защиты (SECTOOLS) упрощает управление защитой системы. Оно содержит различные опции и команды.

Настройка контроля за действиями

Контроль за действиями позволяет регистрировать sj.snbz? связанные с защитой, в журнале QAUDJRN.

Описание:

Задача:

Настройка системы для регистрации событий, влияющих на защиту, в журнале QAUDJRN.

Средства для ее решения:

CRTJRNRCV
CRTJRN QSYS/QAUDJRN
WRKSYSVAL *SEC
CHGOBJAUD
CHGDLOAUD
CHGUSRAUD

Права доступа:

Права доступа *ADD к библиотеке QSYS и
к библиотеке получателя журнала
Специальные права доступа *AUDIT

Запись в журнале:

- CO (создание объекта)
- SV (изменение системного значения)
- AD (изменение параметров контроля за объектами и пользователями)

Прим.: Системное значение QAUDCTL можно изменить только в том случае, если журнал QSYS/QAUDJRN уже существует. В противном случае функция контроля не найдет журнал.

Для того чтобы настроить контроль за действиями, выполните приведенные ниже инструкции. Для выполнения этих действий необходимы специальные права доступа *AUDIT.

1. С помощью команды Создать получатель журнала (CRTJRNRCV) создайте получателя журнала в библиотеке по вашему выбору. В данном примере для получателей журнала используется библиотека с именем JRNLIB.

```
CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +
           THRESHOLD(100000) AUT(*EXCLUDE)  +
           TEXT('Получатель журнала контроля за действиями')
```

- a. Создайте получатель журнала в библиотеке, которая регулярно сохраняется. **Не** размещайте получатель в библиотеке QSYS, даже если в ней будет находиться журнал.
- b. Выберите для получателя журнала имя, которое в дальнейшем может применяться для создания имен других получателей в соответствии с соглашением о присвоении имен. Например, можно выбрать имя AUDRCV0001. Для того чтобы при замене получателей журнала им присваивались имена в соответствии с соглашением о присвоении имен, укажите значение *GEN.

Соглашение такого типа может применяться и в случае, если вы выберете автоматическую замену получателей журнала.

- c. Задайте для получателя журнала пороговые значения с учетом размера и загруженности системы. Максимальный размер зависит от числа транзакций в вашей системе и от того, сколько действий в ней контролируется. Если в системе поддерживается автоматическая замена получателей, то максимальный размер получателя журнала должен быть не менее 100000 Кб. Подробная информация о размере получателя журнала содержится в разделе Управление журналом.
- d. Для того чтобы ограничить доступ к хранящейся в журнале информации, укажите в параметре AUT значение *EXCLUDE.

2. Создайте журнал QSYS/QAUDJRN с помощью команды Создать журнал (CRTJRN) :

```
CRTJRN  JRN(QSYS/QAUDJRN) +
        JRNRCV(JRNLIB/AUDRCV0001) +
        MNGRCV(*SYSTEM) DLTRCV(*NO) +
        AUT(*EXCLUDE) TEXT('Журнал контроля')
```

- Необходимо указать имя QSYS/QAUDJRN.
- Укажите имя получателя журнала, который вы создали на предыдущем шаге.
- Для того чтобы ограничить доступ к хранящейся в журнале информации, укажите в параметре AUT значение *EXCLUDE. Для создания журнала вам необходимы права на добавление объектов в библиотеку QSYS.
- С помощью параметра *Управление получателем* (MNGRCV) укажите системе, что она должна заменять получатель журнала и подключать новый, когда размер текущего получателя достигает порогового значения, указанного при его создании. При выборе этой опции вам не придется отключать получателей с помощью команды CHGJRN, а затем создавать и подключать новых получателей журнала вручную.
- Не задавайте опцию удаления отключенных получателей. Укажите DLTRCV(*NO) (это значение по умолчанию). Получатели QAUDJRN хранят информацию контроля, в которой зафиксированы действия, выполнявшиеся в системе. Перед тем как удалять получателей из системы, убедитесь, что они сохранены.

Подробная информация о работе с журналами и получателями журналов приведена в разделе Управление журналом.

3. С помощью команды WRKSYSVAL установите системное значение QAUDLVL (уровень контроля) или QAUDLVL2 (расширенный уровень контроля). Эти системные значения определяют набор действий,

которые будут регистрироваться в журнале контроля для всех пользователей. Информация приведена в разделе “Планирование контроля действий” на стр. 278.

4. С помощью команды CHGUSRAUD настройте параметры контроля действий для отдельных пользователей (если это необходимо). Информация приведена в разделе “Планирование контроля действий” на стр. 278.
5. С помощью команд CHGOBJAUD, CHGAUD и CHGDLOAUD установите контроль за объектом для отдельных объектов. Информация приведена в разделе “Планирование контроля доступа к объектам” на стр. 304.
6. С помощью команды CHGUSRAUD установите контроль за объектами для отдельных пользователей, если это необходимо.
7. Задайте системное значение QAUDENDACN, чтобы определить действие системы в случае, если ей не удастся получить доступ к журналу контроля. Информация приведена в разделе “Действие при сбое контроля” на стр. 307.
8. Задайте системное значение QAUDFRCLVL, чтобы определить периодичность сохранения записей журнала контроля во вспомогательной памяти. Информация приведена в разделе “Предотвращение потерь данных контроля” на стр. 306.
9. Включите контроль, указав системное значение QAUDCTL, отличное от *NONE.

Системное значение QAUDCTL можно изменить только в том случае, если журнал QSYS/QAUDJRN уже существует. При запуске контроля система попытается добавить запись в журнал контроля. Если ей не удастся это сделать, то будет показано сообщение, а контроль запущен не будет.

Управление журналом контроля и получателями журнала

Система содержит механизм управления журналом контроля и получателями журнала. В этом разделе описаны методы контроля защиты в системе.

Журнал контроля QSYS/QAUDJRN используется только для контроля за действиями. В нем не следует сохранять информацию об объектах. Его не следует использовать для управления фиксацией. Кроме того, в него не следует добавлять пользовательские записи с помощью команды Отправить запись журнала (SNDJRNE) или API Отправить запись журнала (QJOSJRNE).

Для того чтобы система в любой момент могла добавить записи в журнал контроля, этот журнал защищается при помощи блокировки. Когда включен контроль (системное значение QAUDCTL не равно *NONE), системное задание-арбитр (QSYSARB) блокирует журнал QSYS/QAUDJRN. Во время контроля над журналом нельзя выполнять некоторые операции, в том числе:

- Команда DLTJRN
- Перемещение журнала
- Восстановление журнала
- Команда WRKJRN

Информация, сохраняемая в записях журнала контроля, описана в книге Приложение F, “Макет записей журнала контроля”, на стр. 593. Код всех записей защиты в журнале контроля равен T. Помимо записей защиты, журнал QAUDJRN содержит системные записи. Это записи с кодом J, которые относятся к программе начальной загрузки (IPL) и общим операциям над получателями журнала (например, сохранение получателей).

Если журнал или получатель поврежден, и в него нельзя добавить контрольные записи, то система выполняет действия, указанные в системном значении QAUDENDACN. Поврежденный журнал контроля или его получатель следует восстанавливать так же, как обычный журнал или получатель.

Рекомендуется настроить автоматическую замену получателей журнала в системе. Укажите значение MNGRCV(*SYSTEM) при создании журнала QAUDJRN или измените параметр журнала на это значение

позднее. Если указано значение MNGRCV(*SYSTEM), то при переполнении получателя система автоматически отключит его, а затем создаст и подключит новый получатель. Это называется *автоматической заменой получателей*.

Если для QAUDJRN указано значение MNGRCV(*USER), то при переполнении получателя в очередь сообщений о переполнении, указанную для журнала, отправляется сообщение. Это сообщение содержит уведомление о том, что размер получателя журнала достиг порогового значения. С помощью команды CHGJRN отключите этот получатель и подключите новый. Это позволит избежать возникновения ошибок *Запись не занесена в журнал*. Для того чтобы после получения сообщения продолжал выполняться контроль за действиями, необходимо запустить команду CHGJRN.

По умолчанию для журнала используется очередь сообщений QSYSOPR. Если в вашей системе в очередь сообщений QSYSOPR поступает большое количество сообщений, рекомендуется связать с журналом QAUDJRN другую очередь сообщений, например AUDMSG. Для отслеживания поступления сообщений в очередь AUDMSG можно использовать программу обработки сообщений. При получении предупреждения о переполнении получателя (CPF7099) можно автоматически подключать новый получатель. Если вы используете опцию автоматической замены получателей, то после завершения автоматической замены журнала в очередь сообщений журнала отправляется сообщение CPF7020. Появление этого сообщения в очереди говорит о том, что можно выполнить сохранение отключенных получателей журнала.

Внимание: Функция автоматической очистки, содержащаяся в меню Операционная поддержка, не очищает получатели журнала QAUDJRN. Для того чтобы избежать переполнения диска, необходимо регулярно отключать, сохранять и удалять получатели QAUDJRN.

Полная информация об управлении журналами и получателями журналов приведена в разделе Управление журналом.

Если журнал QAUDJRN не существует, то он создается во время IPL. При этом устанавливается системное значение QAUDCTL, отличное от *NONE. Это происходит только в исключительных случаях, например при замене диска или очистке пула вспомогательной памяти.

Информация, связанная с данной

Управление журналами

Сохранение и удаление получателей журналов контроля

Необходимо регулярно отключать текущий получатель и подключать новый получатель журнала контроля.

Описание:

Задача:

Подключение нового получателя журнала; сохранение и удаление старого получателя

Средства для ее решения:

- CHGJRN QSYS/QAUDJRN JRNRCV(*GEN)
- JRNRCV(*GEN) SAVOBJ (сохранение старого получателя)
- DLTJRNRCV (удаление старого получателя)

Права доступа:

Права доступа *ALL к получателю журнала и права доступа *USE к журналу.

Запись в журнале:

J (системная запись в QAUDJRN)

Прим.: Выберите время, когда система загружена меньше всего.

Существуют две причины, по которым необходимо регулярно отключать текущий получатель и подключать новый получатель журнала контроля:

- Анализировать записи журнала гораздо легче, если они охватывают ограниченный, поддающийся контролю период времени.
- Получатели большого размера не только занимают значительный объем вспомогательной памяти, но и приводят к снижению производительности системы.

Рекомендуется настроить автоматическое управление получателями. Это можно указать в параметре *Управление получателем* при создании журнала.

Если вы настроили контроль действий и контроль объектов для отслеживания многих событий, вам может потребоваться настроить большой пороговый размер для получателя журнала. Если вы управляете получателями вручную, рекомендуется заменять получатели журнала несколько раз в день. Если вы отслеживаете небольшое число событий, рекомендуется заменять получатели в соответствии с планом резервного копирования библиотеки, содержащей получатель журнала.

Для отключения старого получателя и подключения нового применяется команда CHGJRN.

Получатели журнала, управляемые системой:

В этом разделе описаны действия по сохранению или удалению получателя журнала.

Если получателями журналов управляет система, то для сохранения всех отключенных получателей QAUDJRN и их удаления необходимо применять следующую процедуру:

1. Введите команду WRKJRNA QAUDJRN. Будет показан получатель, подключенный в данный момент. Не сохраняйте и не удаляйте его.
2. Для работы с каталогом этого получателя нажмите клавишу F15. Будет показан список всех получателей, которые были связаны с журналом, и их состояние.
3. Используйте команду SAVOBJ для сохранения получателей. Не принимайте текущий получатель.
4. С помощью команды DLTJRNRCV удалите каждый получатель после того, как сохраните его.

Вместо выполнения этой процедуры можно отслеживать появление сообщения CPF7020 в очереди сообщений журнала. Это сообщение свидетельствует о том, что система успешно заменила получатель, и его можно сохранить.

Информация, связанная с данной



Резервное копирование и восстановление

Получатели журналов, управляемые пользователями:

В этом разделе описаны операции с получателями журналов, выполняемые вручную, такие как отсоединение, сохранение или удаление.

Если вы вручную управляете получателями журналов, то для отключения, сохранения и удаления получателя необходимо выполнить следующие действия:

1. Введите команду CHGJRN JRN(QAUDJRN) JRNRCV(*GEN). Эта команда выполняет следующие действия:
 - a. Отключает текущий получатель.
 - b. Создает новый получатель со следующим по порядку номером.
 - c. Подключает новый получатель к журналу.

Например, если текущий получатель - AUDRCV0003, то система создает и подключает новый получатель с именем AUDRCV0004.

Узнайте, какой получатель журнала подключен в данный момент, с помощью команды Работа с атрибутами журнала (WRKJRNA): WRKJRNA QAUDJRN.

2. Для сохранения отключенного получателя журнала контроля введите команду Сохранить объект (SAVOBJ). Укажите тип объекта *JRNRCV.

- Удалите получатель с помощью команды Удалить получатель журнала (DLTJRNRCV). При попытке удалить несохраненный получатель журнала будет показано предупреждающее сообщение.

Выключение функции контроля

Функцию контроля рекомендуется применять лишь время от времени. Например, ее можно запустить на время тестирования нового приложения. Или же вы можете применять эту функцию для ежеквартального контроля за действиями.

Для выключения функции контроля выполните следующие действия:

- С помощью команды WRKSYSVAL измените системное значение QAUDCTL на *NONE. При этом система прекратит регистрировать в журнале какие-либо события, влияющие на защиту.
- С помощью команды CHGJRN отключите текущий получатель журнала.
- С помощью команд SAVOBJ и DLTJRNRCV сохраните и удалите отключенный получатель.
- Как только системное значение QAUDCTL будет изменено на *NONE, журнал QAUDJRN может быть удален. Однако, если вы планируете в дальнейшем возобновить работу функции контроля за действиями, рекомендуется оставить журнал QAUDJRN в системе.

Если для журнала QAUDJRN был задан параметр MNGRCV(*SYSTEM), то во время IPL система отключит получатель этого журнала и подключит новый, независимо от того, активна функция контроля или нет. Эти получатели необходимо удалять. Сохранять их перед удалением необязательно, так как они не содержат никаких записей контроля.

Анализ записей журнала контроля

После того как вы настроили функцию контроля за действиями, вы можете анализировать регистрируемые события несколькими способами.

- Просмотр выбранных записей на своей рабочей станции с помощью команды Показать журнал (DSPJRN).
- Копирование выбранных записей в файлы вывода с помощью команды Скопировать записи журнала контроля (CPYAUDJRNE) или команды Показать журнал (DSPJRN) и затем анализируя их с помощью инструмента запросов или соответствующей программы
- Команда Показать записи журнала контроля (DSPAUDJRNE).

Примечание: Фирма IBM больше не предоставляет обновления команды DSPAUDJRNE. Эта команда поддерживает не все типы записей контроля и показывает не все поля поддерживаемых записей.

- Для получения записей в том виде, в каком они содержатся в журнале QAUDJRN, используйте команду Получить запись журнала (RCVJRNE).

Просмотр записей журнала контроля

Описание:

Задача:

Просмотр записей QAUDJRN

Средства для ее решения:

DSPJRN (команда Показать журнал)

Права доступа:

Права доступа *USE к журналу QSYS/QAUDJRN; права доступа *USE к получателю журнала

Команда Показать журнал (DSPJRN) позволяет просматривать выбранные записи журнала на своей рабочей станции. Для просмотра записей журнала выполните следующие действия:

1. Введите DSPJRN QAUDJRN и нажмите F4. В приглашении вы можете ввести информацию о том, какие записи должны быть показаны. Например, вы можете просмотреть все записи в каком-нибудь диапазоне дат, или только определенный тип записей, например записи о неудачных попытках входа в систему (тип записи PW).

По умолчанию будут показаны записи только из подключенного получателя. Для того чтобы просмотреть записи из всех получателей, связанных с журналом QAUDJRN, включая текущий получатель, задайте параметр RCVRNG(*CURCHAIN).

2. После нажатия клавиши Enter появится меню Показать записи журнала:

```

Показать записи журнала

Журнал . . . . . : QAUDJRN      Библиотека . . . . . : QSYS
Наибольший порядковый номер в меню. . . . . : 000000000000000012
Введите опции и нажмите Enter.
5=Показать всю запись

Опц      Номер Код  Тип  Объект      Библиотека  Задание      Время
      1   J   PR   Объект      Библиотека  SCPF         10:24:55
      2   T   CA
      3   T   CO
      4   T   CA
      5   T   CO
      6   T   CA
      7   T   CO
      8   T   CA
      9   T   CO
     10   T   CA
     11   T   CO
     12   T   CA
                                SCPF         10:24:57
                                SCPF         10:24:57
                                SCPF         10:24:57
                                F3=Выход      F12=Отмена

```

3. Опция 5 (Показать всю запись) позволяет просмотреть информацию о конкретной записи:

```

Показать запись журнала

Объект . . . . . :      Библиотека . . . . . :
Элемент . . . . . :
Неполные данные . . : Нет      Сокращенные данные : *None
Порядковый номер . . : 1198
Код . . . . . : T - Запись контрольного журнала
Тип . . . . . : CO - Создать объект

Содержимое записи
Столбец *...+...1...+...2...+...3...+...4...+...5
00001 'NISAVLDCK QSYS *PGM CLE '
00051 ' '
00101 ' '
00151 ' '
00201 ' '
00251 ' '
00301 ' '

Еще... Для
продолжения нажмите Enter.
F3=Выход F6=Показать только данных о записях
F10=Показать только сведения о записях F12=Отмена F24=Доп. клавиши

```

4. Если содержательная часть записи очень велика, то можно пользоваться клавишей F6 (Показать только содержимое записи). При необходимости можно просмотреть содержимое записи в шестнадцатеричном формате. С помощью клавиши F10 можно просмотреть сведения о записи без содержимого записи. Форматы разных типов записей журнала QAUDJRN описаны в разделе Приложение F, “Макет записей журнала контроля”, на стр. 593.

Анализ записей журнала контроля с помощью утилиты запроса или программы

Описание:

Задача:

Просмотр или печать выбранной информации из записей журнала.

Средства для ее решения:

DSPJRN OUTPUT(*OUTFILE), Создать запрос или программу, либо Запустить запрос или программу

Права доступа:

Права доступа *USE к журналу QSYS/QAUDJRN и к получателю журнала и права доступа *ADD к библиотеке файла вывода

С помощью команды Показать журнал (DSPJRN) можно скопировать выбранные записи из получателей журнала в файл вывода. Информацию из файла вывода можно просмотреть с помощью программы или запроса.

В параметре вывода команды DSPJRN укажите значение *OUTFILE. Будут показаны поля, в которых можно задать параметры файла вывода:

```
Показать журнал (DSPJRN)
Введите опции, нажмите Enter.
:
Вывод . . . . . > *OUTFILE
Формат файла вывода . . . . . *TYPE5
Файл для получения вывода . . . dspjrnout
Библиотека . . . . . mylib
Опции элемента вывода:
  Элемент для получения вывода . . . *FIRST
  Замена или добавление записей . . . *REPLACE
Длина данных записи:
  Формат данных поля . . . . . *OUTFILFMT
Длина поля переменной длины
Выделенная длина . . . . .
```

Все записи о событиях в журнале контроля содержат одинаковые заголовки столбцов, такие как тип записи, дата создания записи и имя задания, послужившего причиной создания записи. Если вы выбрали формат файла вывода *TYPE5, то эти поля можно определить с помощью QADSPJR5 (с форматом записи QJORDJE5). Дополнительная информация приведена в разделе “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594.

Информация о других записях и соответствующих форматах файла вывода приведена в разделе Приложение F, “Макет записей журнала контроля”, на стр. 593.

Если вы хотите детально проанализировать записи определенного типа, используйте один из существующих модельных файлов вывода базы данных. В Табл. 132 на стр. 285 приведены имена модельных файлов вывода базы данных для разных типов записей журнала. В Приложение F, “Макет записей журнала контроля”, на стр. 593 приведены макеты файлов для всех модельных файлов вывода базы данных.

Например, для того чтобы создать в библиотеке QGPL файл вывода с именем AUDJRNAF5, который содержит только записи о нарушениях прав доступа, выполните следующие действия:

1. Создайте пустой файл вывода с форматом, определенным для записей журнала AF:

```
CRTDUPOBJ OBJ(QASYAFJ5) FROMLIB(QSYS) +
  OBJTYPE(*FILE) TOLIB(QGPL) NEWOBJ(AUDJRNAF5)
```

2. С помощью команды DSPJRN скопируйте выбранные записи журнала в этот файл вывода:

```
DSPJRN JRN(QAUDJRN) ... +
JRNCDE(T) ENTTYP(AF) OUTPUT(*OUTFILE) +
OUTFILFMT(*TYPE5) OUTFILE(QGPL/AUDJRNF5)
```

3. Для анализа информации в файле AUDJRNF5 запустите Query или соответствующую программу.

Ниже приведено несколько примеров использования информации из журнала QAUDJRN:

- Если вы подозреваете, что кто-то пытается взломать вашу систему:
 1. Убедитесь, что системное значение QAUDLVL содержит *AUTFAIL.
 2. С помощью команды CRTDUPOBJ создайте пустой файл вывода с форматом QASYPWJ5.
 3. Если в меню входа в систему кто-то вводит неправильный ИД пользователя или пароль, в журнал добавляется запись PW. С помощью команды DSPJRN скопируйте записи типа PW в созданный файл вывода.
 4. Создайте программу обработки запроса, которая показывает или печатает для каждой записи журнала дату, время и рабочую станцию. Эта информация поможет вам определить, где и когда предпринималась попытка несанкционированного доступа в систему.
- Если вы хотите проверить надежность защиты ресурса, определенного для нового приложения:
 1. Убедитесь, что системное значение QAUDLVL содержит *AUTFAIL.
 2. Выполните тестирование приложения с разными ИД пользователя.
 3. С помощью команды CRTDUPOBJ создайте пустой файл вывода с форматом QASYAFJ5.
 4. С помощью команды DSPJRN скопируйте в этот файл записи типа AF.
 5. Создайте программу обработки запроса, которая показывает или печатает информацию об объекте, задании и пользователе. Эта информация поможет вам определить, какие пользователи или функции приложения могут привести к нарушениям прав доступа.
- Если вы планируете выполнить переход на уровень защиты 40:
 1. Убедитесь, что системное значение QAUDLVL содержит *PGMFAIL и *AUTFAIL.
 2. С помощью команды CRTDUPOBJ создайте пустой файл вывода с форматом QASYAFJ5.
 3. С помощью команды DSPJRN скопируйте в этот файл записи типа AF.
 4. Создайте программу обработки запроса, которая будет выбирать записи с типом нарушений, ожидаемых при тестировании приложения, а также печатать информацию о задании и программе, приводящих к появлению этих записей.

Примечание: В Табл. 132 на стр. 285 показано, какие записи заносятся в журнал для каждого сообщения о нарушении прав доступа.

Сравнительное описание поля Дата и время изменения объекта и записей контроля

Отчеты, создаваемые с целью обнаружения изменений в программах и других объектах, иногда строятся на основе поля Дата и время изменения конкретного объекта, а не информации из журнала контроля. В следующем списке указаны причины, по которым дата в объекте и дата в источнике объекта могут не совпадать.

- С помощью команды CHGPGM выполняется принудительное повторное создание программы. Это вызывает обновление поля Дата и время изменения в программе. Эта операция создает запись контроля с кодом ZC (изменение объекта).
- С помощью API Подписать объект (QYDOSGNO) выполняется добавление цифровой подписи в программу или команду. Это вызывает обновление поля Дата и время изменения в программе или команде. Эта операция создает контрольную запись с кодом ZC.

Операционная система может также автоматически обновлять поле Дата и время изменения объекта в следующих ситуациях:

- Если у пользовательского профайла есть частные права доступа к объекту, то при удалении этого объекта система обновляет поле Дата и время изменения в этом пользовательском профайле, поскольку она удаляет эти частные права доступа.
- Если на момент удаления объекта включен контроль, то для удаленного объекта создается запись контроля с кодом DO (операция удаления).
- Поскольку система автоматически обновляет каждый пользовательский профайл, у которого есть частные права доступа к удаленному объекту, записи контроля для таких профайлов не создаются, хотя поля Дата и время изменения в таких профайлах обновляются.

Отслеживать изменения объектов, выполняемые пользователями с помощью обычных системных интерфейсов, можно с помощью журнала контроля. Отчеты об изменениях в объектах, основанные исключительно на поле Дата и время изменения объекта, не могут дать полной информации.

Не используйте поле Дата/Время в общих операциях контроля

Основной принцип при выборе объектов для контроля в i5/OS заключается в том, чтобы контролировать действия пользователей, относящиеся к защите. Другой принцип заключается в том, чтобы не создавать записи контроля для тех операций, которые операционная система выполняет автоматически. Однако в некоторых случаях контроль за такими автоматическими операциями может быть необходим, если операционная система выполняет эту операцию с помощью функции, применяемой также и пользователями.

Поле Дата и время изменения в объекте и записи контроля служат разным целям. Основное предназначение поля Дата и время изменения - указывать, когда изменился объект. Поле Дата и время изменения не указывает, какие конкретно изменения произошли в объекте и кто внес изменение. Чаще всего это поле применяется в качестве индикатора необходимости сохранения объекта для команды Сохранить измененные объекты (SAVCHGOBJ). Команде SAVCHGOBJ не нужна информация о том, когда произошло последнее изменение; ей достаточно указания на то, что объект изменился с момента последнего сохранения. Это позволяет повысить производительность при работе с файлами баз данных. Поле Дата и время изменения обновляется только при первом изменении файла после его последнего сохранения. Если бы поле Дата и время изменения обновлялось при каждом обновлении, добавлении или удалении записей в файле, то это существенно снизило бы производительность.

Другие способы контроля эффективности защиты системы

Основной источник информации о событиях в системе, влияющих на ее защиту - это журнал контроля (QAUDJRN). Ниже рассматриваются другие способы отслеживания событий, влияющих на защиту системы, и параметров защиты.

Дополнительную информацию можно найти в разделе Приложение G, “Команды и меню защиты”, на стр. 749. В этом разделе приведены примеры применения команд и информация о меню утилит защиты.

Отслеживание сообщений о попытках нарушения защиты

Некоторые события, влияющие на защиту, например неудачные попытки входа в систему, приводят к появлению соответствующего сообщения в очереди сообщений QSYSOPR. Для этих сообщений можно создать отдельную очередь с именем QSYSMSG в библиотеке QSYS.

Если вы создадите очередь QSYSMSG в библиотеке QSYS, то сообщения о наиболее важных событиях в системе будут отправляться не только в эту очередь, но и в очередь QSYSOPR. Появление сообщений в очереди QSYSMSG может отслеживаться независимо программой или системным оператором. Такой подход обеспечивает дополнительную защиту ресурсов вашей системы. Из-за того что в очередь QSYSOPR направляется большое число сообщений, некоторые важные сообщения могут остаться незамеченными.

Работа с протоколом хронологии

В протоколе QHST регистрируются не все сообщения об ошибках доступа и нарушении целостности. Эти сообщения описаны здесь.

Некоторые события, влияющие на защиту (например, превышение числа неудачных попыток входа в систему, определенного в системном значении QMAXSIGN), приводят к появлению сообщения в протоколе хронологии (QHST). Коды таких сообщений находятся в диапазоне от 2200 до 22FF. Эти сообщения имеют префикс CPI, CPF, CPC, CPD и CPA.

В лицензионной программе i5/OS V2R3 и более поздних выпусков некоторые сообщения о нарушениях прав доступа и целостности не отправляются в протокол хронологии QHST. Вся информация, которая прежде была доступна в протоколе QHST, может быть получена из журнала контроля за действиями. Сохранение информации в журнале контроля меньше влияет на производительность системы. Кроме того, журнал контроля предоставляет более подробную информацию о связанных с защитой событиях, чем протокол QHST. Протокол QHST не следует рассматривать как источник полной информации о нарушениях защиты. Вместо него следует использовать функции контроля за действиями.

В протокол QHST больше не заносятся следующие сообщения:

- CPF2218. Соответствующие события регистрируются в журнале контроля при наличии значения *AUTFAIL в системном значении QAUDLVL.
- CPF2240. Соответствующие события регистрируются в журнале контроля при наличии значения *AUTFAIL в системном значении QAUDLVL.
- CPF2220. Соответствующие события регистрируются в журнале контроля при наличии значения *AUTFAIL в системном значении QAUDLVL.
- CPF4AAE. Соответствующие события регистрируются в журнале контроля при наличии значения *AUTFAIL в системном значении QAUDLVL.
- CPF2246. Соответствующие события регистрируются в журнале контроля при наличии значения *AUTFAIL в системном значении QAUDLVL.

Применение журналов для отслеживания операций с объектами

Если системное значение QAUDLVL содержит опцию *AUTFAIL для контроля за действиями в системе, то в журнал контроля заносятся записи о всех неудачных попытках входа в систему. Дополнительно можно настроить контроль за наиболее важными объектами системы, чтобы в журнале регистрировались все успешные обращения к этим объектам.

Запись добавляется в журнал контроля только при обращении (доступе) к объекту. В журнале не регистрируются все транзакции для этого объекта. Для наиболее важных объектов рекомендуется собирать подробную информацию, позволяющую узнать, к каким именно данным был получен доступ и какие данные были изменены. Такую информацию можно получить, включив ведение журнала объектов. Регистрация операций с объектами в журнале применяется главным образом для контроля за целостностью и восстановления объектов. В разделе Управление журналом приведен список типов объектов, доступ к которым может регистрироваться в журнале, а также описание информации, которая заносится в журнал для каждого типа объекта. На основе этой информации системный администратор или администратор контроля может определить, были ли изменены объекты. Информацию о работе с объектами не следует сохранять в журнале QAUDJRN.

Записи журнала могут включать следующую информацию:

- Имя задания, имя пользователя и время обращения к объекту
- Старое и новое значение при изменении объекта
- Время, когда объект был открыт, закрыт, изменен, сохранен, создан, удален и т.п.

Ни пользователи, ни системные администраторы не могут изменять записи журнала. Заполненный журнал или получатель журнала может быть удален, но это легко обнаружить.

Если вы ведете журнал для файла базы данных, области данных, очереди данных, библиотеки или объекта интегрированной файловой системы, то с помощью команды DSPJRN вы можете напечатать все изменения, произошедшие в данном объекте. Ниже приведено несколько примеров:

| Введите следующую команду для конкретного файла базы данных.

```
| DSPJRN JRN(библиотека/журнал) +  
| FILE(библиотека/файл) OUTPUT(*PRINT)
```

| Введите следующую команду для конкретной области данных.

```
| DSPJRN JRN(библиотека/журнал) +  
| OBJ((библиотека/имя_объекта *DTAARA)) OUTPUT(*PRINT)
```

| Введите следующую команду для конкретной очереди данных.

```
| DSPJRN JRN(библиотека/журнал) +  
| OBJ((библиотека/имя_объекта *DTAQ)) OUTPUT(*PRINT)
```

| Введите следующую команду для конкретного объекта интегрированной файловой системы.

```
| DSPJRN JRN(библиотека/журнал) +  
| OBJPATH(('путь')) OUTPUT(*PRINT)
```

| Введите следующую команду для библиотеки.

```
| DSPJRN JRN(библиотека/журнал) +  
| OBJ(*LIBL/библиотека *LIB) OUTPUT(*PRINT)
```

Например, если для записи информации о файле CUSTFILE из библиотеки CUSTLIB используется журнал JRNCUST из той же библиотеки CUSTLIB, то команда выглядит так:

```
DSPJRN JRN(CUSTLIB/JRNCUST) +  
FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

Затем вы можете создать файл вывода и извлечь из него все записи об определенном объекте, создав запрос или воспользовавшись SQL.

Введите следующую команду для создания файла вывода для конкретного файла базы данных.

```
DSPJRN JRN(библиотека/журнал) +  
FILE(библиотека/имя_файла) +  
OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(библиотека/файл_вывода) ENTDTALEN(*CALC)
```

Введите следующую команду для создания файла вывода для конкретной области данных.

```
DSPJRN JRN(библиотека/журнал) +  
OBJ((библиотека/имя_объекта *DTAARA)) +  
OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(библиотека/файл_вывода) ENTDTALEN(*CALC)
```

Введите следующую команду для создания файла вывода для конкретной очереди данных.

```
DSPJRN JRN(библиотека/журнал) +  
OBJ((библиотека/имя_объекта *DTAQ)) +  
OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(библиотека/файл_вывода) ENTDTALEN(*CALC)
```

Введите следующую команду для создания файла вывода для конкретного объекта интегрированной файловой системы.

```
DSPJRN JRN(библиотека/журнал) +  
OBJPATH(('путь')) +  
OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(библиотека/файл_вывода) ENTDTALEN(*CALC)
```

Введите следующую команду для создания файла вывода для конкретной библиотеки.

```
| DSPJRN JRN(библиотека/журнал) +  
| OBJ((*LIBL/библиотека *LIB)) +  
| OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(библиотека/файл_вывода) ENTDTALEN(*CALC)
```

Для того чтобы просмотреть список всех журналов в системе, введите команду Работа с журналом (WRKJRN). Для того чтобы определить, для каких объектов ведется тот или иной журнал, введите команду Работа с атрибутами журнала (WRKJRNA).

Информация, связанная с данной

Управление журналами

Анализ пользовательских профайлов

Команда Показать пользователей с правами доступа (DSPAUTUSR) позволяет просмотреть или напечатать полный список пользователей системы.

Этот список можно упорядочить по имени профайла или имени профайла группы. Ниже приведен пример списка профайлов групп.

Показать пользователей с правами доступа				
Профайл группы	Пользоват. профайл	Последнее изменение пароля	Нет пароля	Текст
DPTSM	ANDERSOR	08/04/0x		Роджер Андерс
	VINCENTM	09/15/0x		Марк Винсент
DPTWH	ANDERSOR	08/04/0x		Роджер Андерс
	WAGNERR	09/06/0x		Роз Вагнер
QSECOFR	JONESS	09/20/0x		Шэрон Джонс
	HARRISOK	08/29/0x		Кен Харрисон
*NO GROUP	DPTSM	09/05/0x	X	Сбыт
	DPTWH	08/13/0x	X	Склад
	RICHARDS	09/05/0x		Джанет Ричардс
	SMITHJ	09/18/0x		Джон Смит

Печать выбранных пользовательских профайлов

Команда Показать пользовательский профайл (DSPUSRPRF) позволяет создать файл вывода, который можно обработать с помощью утилиты запросов.

```
DSPUSRPRF USRPRF(*ALL) + TYPE(*BASIC) OUTPUT(*OUTFILE)
```

Используя утилиту запросов, можно создать различные отчеты на основе файла вывода, например:

- Список пользователей, у которых есть специальные права доступа *ALLOBJ и *SPLCTL.
- Список пользователей, упорядоченный по имени профайла (им могут быть начальная программа или класс пользователя).

Вы можете создать программы обработки запросов, создающие различные отчеты на основе файла вывода. Например:

- Список пользователей со специальными правами доступа (все записи, в которых поле UPSPAU не равно *NONE).
- Список пользователей с правами на выполнение команд (все записи, в которых поле *Ограничение возможностей*, называемое UPLTSP в модельном файле вывода базы данных, равно *NO или *PARTIAL).
- Список всех пользователей, для которых определено начальное меню или начальная программа.
- Список неактивных пользователей (по дате последнего входа в систему).
- Список всех пользователей, у которых нет пароля для работы на уровне пароля 0 и 1 (все записи, в которых поле пароля для уровня 0 или 1, называемое UPENPW в модельном файле вывода базы данных, равно N).
- Список всех пользователей, у которых есть пароль для работы на уровне пароля 2 и 3 (все записи, в которых поле пароля для уровня 2 или 3, называемое UPENPH в модельном файле вывода базы данных, равно Y).

Просмотр больших пользовательских профайлов

Иногда требуется оценить эффективность больших пользовательских профайлов. Если в системе существует много пользовательских профайлов с большим числом прав доступа, то выбранную стратегию защиты нельзя признать удачной.

Ниже описан один из способов обнаружения и проверки пользовательских профайлов большого размера.

1. Создайте файл вывода, содержащий информацию обо всех пользовательских профайлах системы, с помощью команды Показать описание объекта (DSPOBJD):
2. Создайте программу обработки запроса, составляющую список имен и размеров пользовательских профайлов, упорядоченный по убыванию размера.
3. Напечатайте подробную информацию о самых больших пользовательских профайлах и убедитесь в том, что права доступа и принадлежащие этим профайлам объекты выбраны правильно:

```
DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +  
        DETAIL(*BASIC) OUTPUT(*OUTFILE)
```

```
DSPUSRPRF USRPRF(имя-пользовательского-профайла) +  
        TYPE(*OBJAUT) OUTPUT(*PRINT)
```

```
DSPUSRPRF USRPRF(имя-пользовательского-профайла) +  
        TYPE(*OBJOWN) OUTPUT(*PRINT)
```

Примечание: Каталоги и объекты каталогов не печатаются. Просмотреть объекты каталогов и библиотек можно с помощью команд WRKOBJOWN и WRKOBJPVT, однако печать в этих командах не предусмотрена.

Размер некоторых пользовательских профайлов, поставляемых фирмой IBM, очень велик из-за большого числа принадлежащих им объектов. Обычно просматривать и анализировать такие профайлы не требуется. Тем не менее, рекомендуется проверить наличие программ, принимающих права доступа пользовательских профайлов фирмы IBM со специальными правами доступа *ALLOBJ, таких как QSECOFR и QSYS. Информация приведена в разделе “Анализ программ, принимающих права доступа” на стр. 322.

Ссылки, связанные с данной

Приложение В, “Пользовательские профайлы, поставляемые IBM”, на стр. 337

В этом разделе содержится информация о пользовательских профайлах, поставляемых вместе с системой. Данные профайлы применяются в качестве владельцев объектов при выполнении различных функций системы. Кроме того, некоторые функции системы выполняются от имени пользовательских профайлов, поставляемых IBM.

Анализ прав доступа к объектам и библиотекам

Можно контролировать права доступа к объектам и библиотекам в системе.

Определить пользователей, у которых есть права доступа к библиотекам в системе, можно следующим образом:

1. Просмотрите список всех библиотек системы с помощью команды DSPOBJD:
DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
2. Просмотрите все права доступа к определенной библиотеке с помощью команды Показать права доступа к объекту (DSPOBJAUT):
DSPOBJAUT OBJ(имя-библиотеки) OBJTYPE(*LIB) +
 ASPDEV(имя-ASP) OUTPUT(*PRINT)
3. Просмотрите список объектов в библиотеке с помощью команды Показать библиотеку (DSPLIB):
DSPLIB LIB(имя-библиотеки) ASPDEV(имя-ASP) OUTPUT(*PRINT)

С помощью этих отчетов вы можете определить, какие объекты содержатся в библиотеке и какие пользователи имеют к ней доступ. При необходимости можно просмотреть права доступа к выбранным объектам библиотеки с помощью команды DSPOBJAUT.

Анализ программ, принимающих права доступа

Программы, принимающие права доступа пользователя со специальными правами доступа *ALLOBJ, представляют угрозу для защиты. Эти программы можно проанализировать для осуществления контроля системы.

Определить и проверить программы, принимающие права доступа, можно следующим способом:

1. Для каждого пользователя со специальными правами доступа *ALLOBJ просмотрите список программ, которые принимают его права доступа, с помощью команды Показать принимающие программы (DSPPGMADP):

```
DSPPGMADP USRPRF(имя-пользовательского-профайла) +  
          OUTPUT(*PRINT)
```

Примечание: Инструкции по просмотру списка пользователей с правами доступа *ALLOBJ приведены в разделе “Печать выбранных пользовательских профайлов” на стр. 320.

2. С помощью команды DSPOBJAUT определите, каким пользователям предоставлен доступ к программе, принимающей права доступа, и какие общие права доступа установлены для этой программы:

```
DSPOBJAUT OBJ(библиотека/программа) +  
          OBJTYPE(*PGM) ASPDEV(имя-ASP) OUTPUT(*PRINT)
```

Примечание: Возможно, параметр типа объекта должен быть равен *PGM, *SQLPKG или *SRVPGM, как указано в отчете DSPPGMADP.

3. Просмотрите исходный код программы и ее описание. С помощью этой информации определите следующее:

- Запрещен ли пользователю программы, принимающей права доступа, доступ к ненужным функциям, например к командной строке.
- Нельзя ли сузить набор прав доступа, принимаемых программой. Приложения, принимающие права доступа, могут использовать один и тот же пользовательский профайл для объектов и программ. Когда пользователь принимает права доступа владельца программы, он получает права доступа *ALL к объектами приложений. Во многих случаях профайлу владельца не нужны специальные права доступа.

4. Проверьте дату последнего изменения программы с помощью команды DSPOBJD:

```
DSPOBJD OBJ(имя_библиотеки/имя_программы) +  
          OBJTYPE(*PGM) ASPDEV(имя_ASP) DETAIL(*FULL)
```

Примечание: Возможно, параметр типа объекта должен быть равен *PGM, *SQLPKG или *SRVPGM, как указано в отчете DSPPGMADP.

Проверка измененных объектов

Наличие в системе измененного объекта обычно указывает на попытку несанкционированного доступа к системе. Вы можете просмотреть список измененных объектов с помощью команды Проверить целостность объекта (CHKOBJTG).

Эту команду рекомендуется запускать после выполнения пользователями следующих операций в системе:

- Восстановление программ
- Применение Специальных сервисных средств (DST)

Эта команда создает файл базы данных с информацией о возможных нарушениях целостности. Вы можете проверить объекты, принадлежащие одному или нескольким профайлам, объекты с указанным шаблоном имени или все объекты в системе. Можно найти те объекты, домен которых был изменен, либо поврежденные объекты. Для обнаружения измененных объектов типа *PGM, *SRVPGM, *MODULE и *SQLPKG можно заново вычислить контрольные значения программ. Можно проверить цифровые подписи объектов. При необходимости можно узнать, не изменились ли библиотеки и команды. Вы также можете

запустить просмотр интегрированной файловой системы или проверить наличие объектов, не прошедших проверку при предыдущем просмотре интегрированной файловой системы.

Для применения команды CHKOBJTG необходимы специальные права доступа *AUDIT. Обработка этой команды может занять много времени, поскольку требуется выполнить много операций поиска и вычислений. Эту команду следует запускать только при низкой загрузке системы. Большинство команд IBM, скопированных из версий младше V5R2, регистрируются в протоколе как нарушения. При установке нового выпуска эти команды необходимо удалять и создавать заново с помощью команды Создать копию объекта (CRTDUPOBJ).

Информация, связанная с данной

Поддержка просмотра

Проверка операционной системы

С помощью API Проверить систему (QYDOCHK) вы можете проверить, не изменились ли ключевые объекты операционной системы с момента их подписания.

Все объекты без подписи и объекты, измененные после создания подписи, сообщаются в разделе ошибок. Допустимыми считаются только подписи, полученные из надежного источника.

Для запуска API QYDOCHK необходимы специальные права доступа *AUDIT. Выполнение этого API может занять много времени, поскольку оно включает в себя большой объем вычислений. Его следует запускать только при низкой загрузке системы.

Ссылки, связанные с данной

API Проверить систему (QYDOCHK)

Контроль действий системного администратора

Рекомендуется сохранять информацию обо всех действиях, выполняемых пользователями со специальными права доступа *ALLOBJ и *SECADM.

Для этого можно установить значение контроля действий в пользовательском профайле:

1. Для каждого пользователя системы со специальными правами доступа *ALLOBJ и *SECADM включите в параметр AUDLVL все значения, которые не вошли в системные значения QAUDLVL и QAUDLVL2. Это можно сделать с помощью команды CHGUSRAUD. Например, если системное значение QAUDLVL содержит значения *AUTFAIL, *PGMFAIL, *PRTDTA и *SECURITY, то настройте параметр AUDLVL для системного администратора с помощью следующей команды:

```
CHGUSRAUD USER(SECUSER) +  
    AUDLVL(*CMD *CREATE *DELETE +  
          *OBJMGT *OFCSRVR *PGMADP +  
          *SAVRST *SERVICE, +  
          *SPLFDTA *SYSMGT)
```

Возможные значения контроля действий описаны в разделе “Контроль действий” на стр. 118.

2. Удалите специальные права доступа *AUDIT из пользовательских профайлов со специальными правами доступа *ALLOBJ и *SECADM. В этом случае пользователи не смогут изменять параметры контроля в своих собственных профайлах.

Из профайла QSECOFR нельзя удалить специальные права доступа. Любой пользователь, вошедший в систему как QSECOFR, может изменить параметры контроля этого профайла. Однако при изменении параметров контроля в профайле QSECOFR с помощью команды CHGUSRAUD в журнал контроля будет занесена запись с типом AD.

Для повышения эффективности контроля системные администраторы (пользователи со специальными правами доступа *ALLOBJ или *SECADM) должны использовать свои собственные профайлы. Пароль профайла QSECOFR не следует сообщать большому числу пользователей.

3. Убедитесь, что системное значение QAUDCTL содержит *AUDLVL.

4. С помощью команды DSPJRN просмотрите записи в журнале контроля. Способы анализа записей описаны в разделе “Анализ записей журнала контроля с помощью утилиты запроса или программы” на стр. 315.

Глава 10. Лицензия на исходный код и отказ от обязательств

IBM предоставляет вам неисключительную лицензию на использование всех примеров программного кода. Разрешается создавать на их основе программный код, необходимый вам.

ПРИ УСЛОВИИ СОБЛЮДЕНИЯ ВСЕХ НЕ ДОПУСКАЮЩИХ ИСКЛЮЧЕНИЙ ГАРАНТИЙ, ПРЕДУСМОТРЕННЫХ ЗАКОНОМ, IBM, РАЗРАБОТЧИКИ ПРОГРАММ И ПОСТАВЩИКИ НЕ ПРЕДОСТАВЛЯЮТ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ ИЛИ ПРИМЕНЕНИЯ ДЛЯ КАКИХ-ЛИБО КОНКРЕТНЫХ ЦЕЛЕЙ.

IBM, РАЗРАБОТЧИКИ ПРОГРАММ ИЛИ ПОСТАВЩИКИ НИ ПРИ КАКИХ УСЛОВИЯХ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА:

1. ПОТЕРЮ ИЛИ ПОВРЕЖДЕНИЕ ДАННЫХ;
2. ПРЯМОЙ, ЧАСТНЫЙ, СВЯЗАННЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ И ВЫЗВАННЫЙ ИМ ЭКОНОМИЧЕСКИЙ УЩЕРБ; ЛИБО
3. УПУЩЕННУЮ ВЫГОДУ, ПОТЕРЮ КЛИЕНТОВ, ДОХОДОВ, ДЕЛОВОЙ РЕПУТАЦИИ ИЛИ ИСТРАЧЕННЫЕ СБЕРЕЖЕНИЯ.

В НЕКОТОРЫХ ЮРИСДИКЦИЯХ НЕ ДОПУСКАЮТСЯ ИСКЛЮЧЕНИЯ ИЛИ ОГРАНИЧЕНИЯ ПРЯМОГО, СВЯЗАННОГО ИЛИ КОСВЕННОГО УЩЕРБА, ПОЭТОМУ НЕКОТОРЫЕ ИЛИ ВСЕ УКАЗАННЫЕ ВЫШЕ ОГРАНИЧЕНИЯ И ИСКЛЮЧЕНИЯ МОГУТ К ВАМ НЕ ОТНОСИТЬСЯ.

Приложение А. Команды для организации защиты

В этом разделе содержится описание системных команд, связанных с организацией защиты. Эти команды можно использовать вместо системных меню, если вы предпочитаете работать с командной строкой. Команды подразделяются на несколько групп в соответствии с выполняемыми задачами.

Более подробная информация об этих командах приведена в разделе Язык (CL). Права доступа к объектам, необходимые для выполнения указанных команд, перечислены в таблицах из раздела Приложение D, “Права доступа, требуемые для объектов, используемых командами”, на стр. 359.

Дополнительная информация о средствах защиты и рекомендации по работе с ними приведены в разделе Настройка работы средств защиты в системе.

Команды для работы с владельцами прав доступа

В этой таблице перечислены команды для работы с владельцами прав доступа.

Таблица 134. Команды для работы с владельцами прав доступа

Команда	Название	Функция
CRTAUTHLR	Создать владельца прав доступа	Позволяет защитить файл до его создания. Владельцы прав доступа применимы только для файлов баз данных, описанных в программе.
DLTAUTHLR	Удалить владельца прав доступа	Позволяет удалить владельца прав доступа. Если существует связанный файл, то информация из владельца прав доступа копируется в этот файл.
DSPAUTHLR	Показать владельца прав доступа	Позволяет показать всех владельцев прав доступа в системе.

Команды для работы со списками прав доступа

Эти команды позволяют выполнять задачи со списками прав доступа.

Таблица 135. Команды для работы со списками прав доступа

Команда	Название	Функция
ADDAUTLE	Добавить запись списка прав доступа	Позволяет добавить пользователя в список прав доступа. Вы должны указать, какие права предоставляются пользователю для доступа ко всем объектам в этом списке.
CHGAUTLE	Изменить запись списка прав доступа	Позволяет изменить права доступа пользователя к объектам из списка прав доступа.
CRTAUTL	Создать список прав доступа	Позволяет создать список прав доступа.
DLTAUTL	Удалить список прав доступа	Позволяет полностью удалить список прав доступа.
DSPAUTL	Показать список прав доступа	Позволяет просмотреть список пользователей и предоставленные пользователям права доступа к списку прав доступа.
DSPAUTLOBJ	Показать объекты списка прав доступа	Позволяет показать список объектов, защищенных с помощью списка прав доступа.

Таблица 135. Команды для работы со списками прав доступа (продолжение)

Команда	Название	Функция
EDTAUTL	Редактировать список прав доступа	Позволяет добавлять пользователей и предоставленные им права в список прав доступа, а также изменять и удалять их из этого списка.
RMVAUTLE	Удалить запись списка прав доступа	Позволяет удалить пользователя из списка прав доступа.
RTVAUTLE	Получить запись списка прав доступа	Применяется в программах на языке CL для получения одного или нескольких значений из списка прав доступа, связанных с пользователем. Эта команда может применяться вместе с командой CHGAUTLE для предоставления пользователю новых прав доступа, в дополнение к тем правам, которые уже есть у пользователя.
WRKAUTL	Работа со списками прав доступа	Позволяет выполнять задачи со списками прав доступа из меню.

Команды прав доступа к объектам и контролю

В этой таблице перечислены команды прав доступа к объектам и контролю.

Таблица 136. Команды прав доступа к объектам и контролю

Команда	Название	Функция
CHGAUD	Изменить параметры контроля	Изменяет значение контроля для объекта.
CHGAUT	Изменить права доступа	Изменяет права доступа пользователей к объектам.
CHGOBJAUD	Изменить параметры контроля объекта	Позволяет включить контроль доступа к объектам.
CHGOBJOWN	Изменить владельца объекта	Изменяет принадлежность объекта.
CHGOBJPGP	Изменить основную группу объекта	Позволяет указать в качестве основной группы объекта другой профайл, либо указать, что у объекта нет основной группы.
CHGOWN	Изменить владельца	Позволяет изменить принадлежность объекта.
CHGPGP	Изменить основную группу	Позволяет указать в качестве основной группы объекта другой профайл, либо указать, что у объекта нет основной группы.
DSPAUT	Показать права доступа	Показывает права доступа пользователей к объекту.
DSPLNK	Показать ссылки	Показывает список имен заданных объектов в каталогах вместе с опциями просмотра дополнительной информации об этих объектах.
DSPOBJAUT	Показать права доступа к объекту	Показывает следующую информацию: владелец объекта, общие и частные права доступа к объекту, имя списка прав доступа, применяемого для защиты этого объекта.
DSPOBJD	Показать описание объекта	Показывает уровень контроля объекта.
EDTOBJAUT	Редактировать права доступа к объекту	Позволяет добавлять, изменять и удалять права доступа пользователя к объекту.
GRTOBJAUT	Предоставить права доступа к объекту	Позволяет предоставить права доступа к объекту, указанному в данной команде, заданным пользователям, всем пользователям (*PUBLIC) или пользователям сылочного объекта.

Таблица 136. Команды прав доступа к объектам и контроля (продолжение)

Команда	Название	Функция
RVKOBJAUT	Аннулировать права доступа к объекту	Позволяет удалить некоторые (или все) права доступа к объектам с указанными именами, предоставленные отдельному пользователю.
WRKAUT	Работа с правами доступа	Позволяет работать с правами доступа к объекту с помощью меню.
WRKLNK	Работа со ссылками	Показывает список имен заданных объектов в каталогах вместе с опциями работы с этими объектами.
WRKOBJ	Работа с объектами	Позволяет работать с правами доступа к объекту с помощью меню.
WRKOBJOWN	Работа с объектами по владельцу	Позволяет работать с объектами, принадлежащими пользовательскому профайлу.
WRKOBJPGP	Работа с объектами по основной группе	Предоставляет меню со списком опций для работы с объектами, профайл которых является профайлом основной группы.
WRKOBJPVT	Работа с объектами по частным правам доступа	Предоставляет меню со списком опций для работы с объектами, к профайлу которых предоставлены частные права доступа.

Команды для работы с паролями

Администратор защиты может присвоить, изменить, проверить или сбросить пароль пользовательского профайла с помощью указанных команд.

Таблица 137. Команды для работы с паролями

Команда	Название	Функция
CHGDSTPWD	Изменить пароль Специальных сервисных средств	Позволяет изменить пароль профайла DST на пароль по умолчанию, поставляемый вместе с системой.
CHGPWD	Смена пароля	Позволяет изменить пароль пользователя.
CHGUSRPRF	Изменить пользовательский профайл	Позволяет изменять значения, указанные в пользовательском профайле, в том числе пароль пользователя.
CHKPWD	Проверить пароль	Позволяет проверить пароль пользователя. Например, если вы хотите, чтобы пользователь еще раз вводил пароль при запуске какого-либо приложения, вы можете указать команду CHKPWD в своей программе на CL для проверки пароля.
CRTUSRPRF ¹	Создать пользовательский профайл	При добавлении пользователя в систему задается пароль этого пользователя.

¹ С помощью команды CRTUSRPRF нельзя создать пользовательский профайл (*USRPRF) в независимом пуле дисков (ASP). Тем не менее, если у пользователя есть частные права доступа к объекту в независимом пуле дисков, он является владельцем объекта в этом пуле или входит в основную группу такого объекта, имя профайла этого пользователя сохраняется в независимом пуле дисков. При перемещении такого пула дисков в другую систему частные права доступа, принадлежность объекта и записи основной группы присваиваются пользовательскому профайлу в новой системе с таким же именем. Если в целевой системе нет такого профайла, то он будет создан. При этом пользователю не предоставляются специальные права доступа, а в качестве пароля указывается значение *NONE.

Команды пользовательского профайла

Администратор защиты применяет описанные команды для работы с пользовательскими профайлами.

Таблица 138. Команды пользовательского профайла

Команда	Название	Функция
CHGPRF	Изменить профайл	Позволяет изменить атрибуты пользовательского профайла.
CHGUSRAUD	Изменить пользовательский контроль	Позволяет настроить контроль за действиями и объектами для пользовательского профайла.
CHGUSRPRF	Изменить пользовательский профайл	Позволяет изменять значения, указанные в пользовательском профайле, например, пароль пользователя, специальные права доступа, начальное меню, текущую библиотеку и максимальное значение приоритета.
CHKOBJTG	Проверить целостность объекта	Проверяет, не повреждены ли объекты, принадлежащие одному или нескольким пользовательским профайлам, или объекты с указанным полным именем.
CRTUSRPRF	Создать пользовательский профайл	Позволяет добавить пользователя в систему и задать для него пароль, специальные права доступа, начальное меню, текущую библиотеку и максимальное значение приоритета.
DLTUSRPRF	Удалить пользовательский профайл	Позволяет удалить пользовательский профайл из системы. Кроме того, позволяет отменить или изменить принадлежность объектов, которые принадлежат удаляемому пользовательскому профайлу.
DMPUSRPRF	Дамп пользовательского профайла	Позволяет создать дамп пользовательского профайла и связанной информации.
DSPAUTUSR	Показать пользователей с правами доступа	Позволяет просмотреть или напечатать следующую информацию для всех пользовательских профайлов в системе: связанный профайл группы (если он существует); установлен ли для профайла пароль, применимый на любом уровне защиты; установлен ли пароль, применимый на разных уровнях; установлен ли пароль для NetServer; дата последнего обновления пароля; описание пользовательского профайла.
DSPSSTUSR	Показать ИД пользователя сервисных средств	Позволяет показать список идентификаторов пользователей сервисных средств. Также может использоваться для показа подробной информации о конкретном ИД пользователя сервисных средств, включая состояние пользователя и его права доступа.
DSPUSRPRF	Показать пользовательский профайл	Позволяет показать пользовательский профайл в различных форматах.
GRTUSRAUT	Предоставить права доступа пользователю	Позволяет скопировать частные права доступа из одного пользовательского профайла в другой.
PRTPRFINT	Печать внутренних данных профайла	Позволяет напечатать отчет о содержимом нескольких записей профайла.
PRTUSRPRF	Печать пользовательского профайла	Анализ пользовательских профайлов, отвечающих указанным критериям.
RTVUSRPRF	Получить пользовательский профайл	Применяется в программах на языке CL для получения и использования одного или нескольких значений, которые хранятся в пользовательском профайле и связаны с ним.

Таблица 138. Команды пользовательского профайла (продолжение)

Команда	Название	Функция
WRKUSRPRF	Работа с пользовательскими профайлами	Позволяет работать с пользовательскими профайлами с помощью меню.

Команды для работы с пользовательским профайлом

В этой таблице перечислены некоторые дополнительные команды, применяемые для работы с пользовательским профайлом. Эти команды позволяют сохранить и восстановить пользовательские профайлы и их атрибуты.

Таблица 139. Команды для работы с пользовательским профайлом

Команда	Название	Функция
DSPPGMADP	Показать принимающие программы	Позволяет просмотреть список программ и пакетов SQL, принимающих права доступа указанного пользовательского профайла.
RSTAUT	Восстановить права доступа	Позволяет восстановить права доступа к объектам, которые были заблокированы пользовательским профайлом в момент его сохранения. Эти права доступа могут быть восстановлены только после восстановления пользовательского профайла командой Восстановить пользовательский профайл (RSTUSRPRF).
RSTUSRPRF	Восстановить пользовательский профайл	Позволяет восстановить пользовательский профайл и его атрибуты. После восстановления пользовательского профайла можно восстановить отдельные права доступа к объектам с помощью команды RSTAUT. Если вы укажете параметр RSTUSRPRF(*ALL), то будут восстановлены все списки прав доступа и владельцы прав доступа.
SAVSECDTA	Сохранить данные защиты	Сохраняет все пользовательские профайлы, списки прав доступа и владельцев прав доступа без использования системы, которая находится в состоянии с ограничениями.
SAVSYS	Сохранить систему	Сохраняет все пользовательские профайлы, списки прав доступа, владельцев прав доступа в системе. При использовании этой команды в системе не должны выполняться никакие другие задания.

Команда контроля

Эти команды позволяют выполнять задачи контроля объектов.

Таблица 140. Команда контроля

Команда	Название	Функция
CHGAUD	Изменить параметры контроля	Позволяет настроить параметры контроля.
CHGDLOAUD	Изменить параметры контроля объекта библиотеки документов	Позволяет включить контроль доступа к объекту библиотеки документов.
CHGOBJAUD	Изменить параметры контроля объекта	Позволяет настроить параметры контроля.
CHGUSRAUD	Изменить пользовательский контроль	Позволяет настроить контроль за действиями и объектами для пользовательского профайла.

Команды для работы с объектами библиотеки документов

В этой таблице перечислены команды для работы с объектами библиотеки документов.

Таблица 141. Команды для работы с объектами библиотеки документов

Команда	Название	Функция
ADDDLOAUT	Добавить права доступа к объекту библиотеки документов	Позволяет предоставить пользователю доступ к документу или папке или защитить документ или папку с помощью списка прав доступа или кода доступа.
CHGDLOAUD	Изменить параметры контроля объекта библиотеки документов	Позволяет указать информацию об уровне контроля объекта библиотеки документов.
CHGDLOAUT	Изменить права доступа к объекту библиотеки документов	Позволяет изменить права доступа к документу или папке.
CHGDLOOWN	Изменить владельца объекта библиотеки документов	Изменяет принадлежность документа или папки.
CHGDLOPGP	Изменить основную группу объекта библиотеки документов	Позволяет изменить основную группу для объекта библиотеки документов.
DSPAUTLDLO	Показать объекты библиотеки документов списка прав доступа	Позволяет просмотреть документы и папки, защищенные указанным списком прав доступа.
DSPDLOAUD	Показать параметры контроля объекта библиотеки документов	Выдает информацию об уровне контроля объекта библиотеки документов.
DSPDLOAUT	Показать права доступа к объекту библиотеки документов	Позволяет показать права доступа к документу или папке.
EDTDLOAUT	Редактировать права доступа к объекту библиотеки документов	Применяется для добавления, изменения или удаления прав доступа пользователя к документу или папке.
GRTUSRPMN	Предоставить права доступа пользователю	Предоставляет пользователю права на работу с документами или папками или на выполнение задач Office от имени другого пользователя.
RMVDLOAUT	Удалить права доступа к объекту библиотеки документов	Позволяет отозвать права доступа пользователя к документам или папкам.
RVKUSRPMN	Аннулировать права доступа пользователя	Отменяет право пользователя (или всех пользователей) работать с документами от имени другого пользователя.

Команды для работы с записью идентификации сервера

Эти команды позволяют показать, добавить, удалить или изменить записи идентификации сервера для пользовательского профайла.

Таблица 142. Команды для работы с записью идентификации сервера

Команда	Название	Функция
ADDSVRAUTE	Добавить запись идентификации сервера	Позволяет добавить информацию идентификации сервера в пользовательский профайл.
CHGSVRAUTE	Изменить запись идентификации сервера	Позволяет изменить существующие записи идентификации сервера для пользовательского профайла.
DSPSVRAUTE	Показать записи идентификации сервера	Позволяет показать записи идентификации сервера для пользовательского профайла.
RMVSVRAUTE	Удалить запись идентификации сервера	Позволяет удалить записи идентификации сервера из пользовательского профайла.

Таблица 142. Команды для работы с записью идентификации сервера (продолжение)

Команда	Название	Функция
С помощью этих команд пользователь может задавать имя пользователя, связанный с ним пароль и имя удаленной системы. Архитектура распределенных реляционных баз данных (DRDA) использует эти записи для обработки запросов к базе данных на удаленном сервере от имени указанного пользователя.		

Команды для работы с системным каталогом рассылки

Эти команды позволяют добавить, удалить или изменить записи в системном каталоге рассылки.

Таблица 143. Команды для работы с системным каталогом рассылки

Команда	Название	Функция
ADDDIRE	Добавить запись каталога	Добавляет новые записи в системный каталог рассылки. Этот каталог содержит информацию о пользователе (ИД пользователя и его адрес), имя системы, имя пользовательского профайла, почтовый адрес и номер телефона.
CHGDIRE	Изменить запись каталога	Позволяет изменить данные, содержащиеся в записи системного каталога рассылки. Системному администратору предоставлены права на обновление любых данных, кроме ИД пользователя, адреса и описания пользователя. Пользователям разрешено обновлять только некоторые поля в собственных записях каталога.
RMVDIRE	Удалить запись каталога	Удаляет запись из системного каталога рассылки. При удалении ИД и адреса пользователя из каталога они также удаляются из всех списков рассылки.
WRKDIRE	Работа с каталогом	Предоставляет набор меню, с помощью которых пользователь может просматривать, добавлять, изменять и удалять записи системного каталога рассылки.

Команды для работы с контрольными списками

Эти две команды предназначены для создания и удаления контрольных списков в библиотеке.

Таблица 144. Команды для работы с контрольными списками

Команда	Название	Функция
CRTVLDL	Создать контрольный список	Позволяет создать объект контрольного списка с записями, содержащими идентификатор, данные, которые будут зашифрованы системой при сохранении записи, а также данные в произвольном формате.
DLTVLDL	Удалить контрольный список	Позволяет удалить указанный контрольный список из библиотеки.

Команды для работы с информацией об использовании функций

Эти команды позволяют изменить или показать информацию об использовании функций.

Таблица 145. Команды для работы с информацией об использовании функций

Команда	Название	Функция
CHGFCNUSG	Изменить права доступа к функции	Изменить информацию об использовании зарегистрированной функции.
DSPFCNUSG	Показать права доступа к функции	Позволяет просмотреть список идентификаторов функций и подробную информацию о правах доступа к отдельной функции.
WRKFCNUSG	Работа с правами доступа к функции	Позволяет просмотреть список идентификаторов функций, а также просмотреть или изменить информацию о правах доступа к функции.

Команды для работы с инструментами защиты контроля

Эти команды предназначены для контроля защиты. Они позволяют работать с записями журнала контроля за действиями и с системными значениями, управляющими защитой.

За дополнительной информацией о средствах защиты обратитесь к разделу Приложение G, “Команды и меню защиты”, на стр. 749.

Таблица 146. Команды для работы с инструментами защиты контроля

Команда	Название	Функция
CHGSECAUD	Изменить параметры контроля за действиями	Позволяет настраивать контроль за действиями и изменять соответствующие системные значения.
CPYAUDJRNE	Скопировать записи журнала контроля	Позволяет скопировать записи из журнала контроля защиты в файлы вывода, которые можно запрашивать. Вы можете выбрать группу записей по типу, по пользователям или по интервалу времени.
DSPAUDJRNE ¹	Показать записи журнала контроля	Позволяет просмотреть или напечатать информацию о записях журнала контроля за действиями. Вы можете выбрать группу записей по типу, по пользователям или по интервалу времени.
DSPSECAUD	Показать параметры контроля за действиями	Позволяет просмотреть информацию о журнале контроля за действиями и о соответствующих системных значениях.
1	Фирма IBM больше не предоставляет обновления команды DSPAUDJRNE. Эта команда поддерживает не все типы записей контроля и показывает не все поля поддерживаемых записей.	

Команды для работы с инструментами защиты прав доступа

Эти команды позволяют выполнять различные задачи печати, связанные с параметрами защиты.

Таблица 147. Команды для работы с инструментами защиты прав доступа

Команда	Название	Функция
PRTJOBDAUT	Печатать права доступа к описаниям заданий	Позволяет напечатать список описаний заданий, общие права доступа к которым отличны от *EXCLUDE. С помощью этой команды можно напечатать список тех описаний заданий, в которых задано имя конкретного пользовательского профайла, и которые доступны всем пользователям системы.
PRT PUBAUT	Печатать объекты, доступные всем пользователям	Позволяет напечатать список объектов указанного типа, общие права доступа к которым отличны от *EXCLUDE.

Таблица 147. Команды для работы с инструментами защиты прав доступа (продолжение)

Команда	Название	Функция
PRTPVTAUT	Печатать частные права доступа	Позволяет напечатать список частных прав доступа к объектам указанного типа.
PRTQAUT	Печатать права доступа к очереди	Позволяет напечатать значения параметров защиты для очередей вывода и очередей заданий системы. Эти параметры определяют пользователей, которые могут просматривать и изменять записи в этих очередях.
PRTSBSDAUT	Печатать права доступа к описанию подсистемы	Позволяет напечатать список описаний подсистем из библиотеки, в которых в записи подсистемы указан пользователь по умолчанию.
PRTTRGPGM	Печатать программы триггера	Позволяет напечатать список программ триггера, связанных с файлами базы данных в подсистеме.
PRTUSROBJ	Печатать пользовательские объекты	Позволяет напечатать список пользовательских объектов (объектов, не поставляемых фирмой IBM), расположенных в библиотеке.

Команды для работы с инструментами защиты системы

Далее описаны команды для работы с инструментами защиты системы .

Таблица 148. Команды для работы с инструментами защиты системы

Команда	Название	Функция
CHGSECA ¹	Изменить атрибуты защиты	Позволяет задать начальные значения для автоматического создания идентификаторов пользователей и групп. Можно указать начальный идентификатор пользователя и начальный идентификатор группы.
CFGSYSSEC	Настроить защиту системы	Позволяет задавать рекомендуемые параметры для системных значений, связанных с защитой. Эта команда дополнительно настраивает контроль за действиями в системе.
CLRSVRSEC	Очистить данные защиты сервера	Позволяет очистить идентификационные данные, связанные с пользовательскими профайлами и записями контрольного списка (*VLDL), которые допускают расшифровку. Примечание: В выпусках младше V5R2 эти данные удалялись при изменении системного значения QRETSVRSEC с '1' на '0'.
DSPSECA	Показать атрибуты защиты	Позволяет просмотреть текущие значения некоторых атрибутов защиты системы и значения, ожидающие вступления в силу.
PRTCMNSEC	Печатать параметры защиты средств связи	Позволяет напечатать атрибуты защиты объектов типа *DEV, *CTL и *LIND.
PRTSYSSECA	Печатать системные атрибуты защиты	Позволяет напечатать список системных значений, связанных с защитой, и сетевых атрибутов. В отчете указано текущее и рекомендуемое значение.
RVKPUBAUT	Аннулировать общие права доступа	Позволяет задать общие права доступа *EXCLUDE для набора команд, требующих защиты.
¹ Для выполнения этой команды необходимы специальные права доступа *SECADM.		

Приложение В. Пользовательские профайлы, поставляемые IBM

В этом разделе содержится информация о пользовательских профайлах, поставляемых вместе с системой. Данные профайлы применяются в качестве владельцев объектов при выполнении различных функций системы. Кроме того, некоторые функции системы выполняются от имени пользовательских профайлов, поставляемых IBM.

Значения по умолчанию для пользовательских профайлов

В этой таблице приведены значения по умолчанию, которые применяются при работе со всеми поставляемыми IBM пользовательскими профайлами и при запуске команды Создать пользовательский профайл (CRTUSRPRF). Порядок параметров совпадает с их очередностью в меню команды Создать пользовательский профайл.

Таблица 149. Значения по умолчанию для пользовательских профайлов

Параметр пользовательского профайла	Применяются значения по умолчанию	
	IBM, поставляемые пользовательские профайлы	Меню Создать профайл пользователя
Пароль (PASSWORD)	*NONE	*USRPRF ⁴
Ограничить срок действия пароля (PWDEXP)	*NO	*NO
Состояние (STATUS)	*ENABLED	*ENABLED
Класс пользователя (USRCLS)	*USER	*USER
Уровень поддержки (ASTLVL)	*SYSVAL	*SYSVAL
Текущая библиотека (CURLIB)	*CRTDFT	*CRTDFT
Начальная программа (INLPGM)	*NONE	*NONE
Начальное меню (INLMNU)	MAIN	MAIN
Библиотека начального меню	*LIBL	*LIBL
Ограничить возможности (LMTCPB)	*NO	*NO
Текст (TEXT)	*BLANK	*BLANK
Специальные права доступа (SPCAUT)	*ALLOBJ ¹ *SAVSYS ¹	*USRCLS ²
Специальная среда (SPCENV)	*SYSVAL	*SYSVAL
Показать информацию о входе в систему (DSPSGNINF)	*SYSVAL	*SYSVAL
Срок действия пароля (PWDEXPITV)	*SYSVAL	*SYSVAL
Ограничить сеансы одним устройством (LMTDEVSSN)	*SYSVAL	*SYSVAL
Буферизация клавиатуры (KBDBUF)	*SYSVAL	*SYSVAL
Максимальный объем памяти (MAXSTG)	*NOMAX	*NOMAX
Ограничение приоритета (PTYLMT)	0	3
Описание задания (JOBID)	QDFTJOBID	QDFTJOBID
Библиотека описания задания	QGPL	*LIBL
Профайл группы (GRPPRF)	*NONE	*NONE
Владелец (OWNER)	*USRPRF	*USRPRF
Права доступа группы (GRPAUT)	*NONE	*NONE

Таблица 149. Значения по умолчанию для пользовательских профайлов (продолжение)

Параметр пользовательского профайла	Применяются значения по умолчанию	
	IBM, поставляемые пользовательские профайлы	Меню Создать профайл пользователя
Тип прав доступа группы (GRPAUTTYR)	*PRIVATE	*PRIVATE
Дополнительные группы (SUPGRPPRF)	*NONE	*NONE
Код учета ресурсов (ACGCDE)	*SYS	*BLANK
Пароль документа (DOCPWD)	*NONE	*NONE
Очередь сообщений (MSGQ)	*USRPRF	*USRPRF
Доставка (DLVRY)	*NOTIFY	*NOTIFY
Уровень серьезности (SEV)	00	00
Принтер (PRTDEV)	*WRKSTN	*WRKSTN
Очередь вывода (OUTQ)	*WRKSTN	*WRKSTN
Программа Attention (ATNPGM)	*NONE	*SYSVAL
Последовательность сортировки (SRTSEQ)	*SYSVAL	*SYSVAL
Идентификатор языка (LANGID)	*SYSVAL	*SYSVAL
Идентификатор страны или региона (CNTRYID)	*SYSVAL	*SYSVAL
Идентификатор набора символов (CCSID)	*SYSVAL	*SYSVAL
Задать атрибуты задания (SETJOBATR)	*SYSVAL	*SYSVAL
Локаль (LOCALE)	*NONE	*SYSVAL
Опция пользователя (USROPT)	*NONE	*NONE
Идентификатор пользователя (UID)	*GEN	*GEN
Идентификатор группы (GID)	*NONE	*NONE
Домашний каталог (HOMEDIR)	*USRPRF	*USRPRF
Права доступа (AUT)	*EXCLUDE	*EXCLUDE
Контроль действий (AUDLVL) ³	*NONE	*NONE
Контроль объектов (OBJAUD) ³	*NONE	*NONE
¹	При изменении уровня защиты системы со значения 10 или 20 на 30 или выше данное значение удаляется.	
²	Если в системе с уровнем защиты 10 создается пользовательский профайл класса *USER, ему предоставляются специальные права доступа *ALLOBJ и *SAVSYS.	
³	Контроль действий и объектов можно настроить с помощью команды CHGUSRAUD.	
⁴	С помощью команды CRTUSRPRF нельзя создать пользовательский профайл (*USRPRF) в независимом пуле дисков. Однако, если пользователь обладает частными правами доступа к объекту из независимого пула дисков, является владельцем такого объекта или входит в состав основной группы этого объекта в независимом пуле дисков, то имя пользовательского профайла хранится в независимом пуле дисков. В случае перемещения независимого пула дисков в другую систему записи о частных правах доступа, принадлежности объектов и основных группах прикрепляются к пользовательскому профайлу с тем же именем в целевой системе. Если в целевой системе нет такого профайла, то он будет создан. При этом пользователю не предоставляются специальные права доступа, а в качестве пароля указывается значение *NONE.	

Пользовательские профайлы, поставляемые IBM

В этой таблице перечислены все поставляемые IBM профайлы, указано их назначение и все значения, отличные от значений по умолчанию для поставляемых IBM пользовательских профайлов.

Примечание:

Пользовательские профайлы, поставляемые IBM, теперь содержат некоторые дополнительные пользовательские профайлы, которые поставляются вместе с лицензионными программами. В таблице указана лишь часть таких профайлов, поэтому список является неполным.

Внимание:

- Пароль пользовательского профайла QSECOFR

После установки системы необходимо изменить пароль пользовательского профайла QSECOFR. Этот пароль является стандартным для всех систем System i, поэтому применение значения по умолчанию делает систему уязвимой. Тем не менее, не следует изменять какие-либо другие значения в поставляемых IBM пользовательских профайлах. Это может привести к сбою в работе функций системы.

- Права доступа поставляемых IBM пользовательских профайлов

Соблюдайте осторожность при удалении прав доступа поставляемых IBM пользовательских профайлов, которые предоставлены им по отношению к объектам, поставляемым вместе с операционной системой. У некоторых поставляемых IBM профайлов есть частные права доступа к объектам, поставляемым вместе с системой. Удаление этих прав доступа может привести к сбоям в работе функций системы.

Таблица 150. IBM, поставляемые пользовательские профайлы

Имя профайла	Название	Параметры, отличающиеся от значений по умолчанию
QADSM	Пользовательский профайл AD SM	<ul style="list-style-type: none">• USERCLS: *SYSOPR• CURLIB: QADSM• TEXT: Профайл AD SM, применяемый сервером AD SM• SPCAUT: *JOBCTL, *SAVSYS• JOB D: QADSM/QADSM• OUTQ: QADSM/QADSM
QAFOWN	Пользовательский профайл AP D	<ul style="list-style-type: none">• USRCLS: *PGMR• SPCAUT: *JOBCTL• JOB D: QADSM/QADSM• TEXT: Внутренний пользовательский профайл AP D
QAFUSR	Пользовательский профайл AP D	<ul style="list-style-type: none">• TEXT: Внутренний пользовательский профайл AP D
QAFDFTUSR	Пользовательский профайл AP D	<ul style="list-style-type: none">• INLPGM: *LIBL/QAFINLPG• LMTCPB: *YES• TEXT: Внутренний пользовательский профайл AP D
QAUTPROF	Пользовательский профайл прав доступа IBM	
QBRMS	Пользовательский профайл BR M	
QCLUMGT	Профайл управления кластерами	<ul style="list-style-type: none">• STATUS: *DISABLED• MSGQ: *NONE• ATNPGM: *NONE

Таблица 150. IBM, поставляемые пользовательские профайлы (продолжение)

Имя профайла	Название	Параметры, отличающиеся от значений по умолчанию
QCLUSTER	Профайл кластера высокой готовности	<ul style="list-style-type: none"> • SPCAUT: *IOSYSCFG
QCOLSRV	Пользовательский профайл служб сбора статистики Централизованного управления	
QDBSHR	Профайл общей базы данных	<ul style="list-style-type: none"> • AUT: *ADD, *DELETE
QDBSHRDO	Профайл общей базы данных	<ul style="list-style-type: none"> • AUT: *ADD, *DELETE
QDFTOWN	Профайл владельца по умолчанию	<ul style="list-style-type: none"> • PTYLMT: 3
QDIRSRV	Пользовательский профайл сервера Сервера каталогов i5/OS	<ul style="list-style-type: none"> • LMTCPB: *YES • JOB: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE
QDLFM	Профайл диспетчера файлов DataLink	<ul style="list-style-type: none"> • SRTSEQ: *HEX
QDOC	Профайл документа	<ul style="list-style-type: none"> • AUT: *CHANGE
QDSNX	Профайл узлового исполнителя в распределенных системах	<ul style="list-style-type: none"> • PTYLMT: 3 • CCSID: *HEX • SRTSEQ: *HEX
QEJBSVR	Пользовательский профайл WebSphere	
QEJB	Пользовательский профайл Enterprise Java	
QFNC	Финансовый профайл	<ul style="list-style-type: none"> • PTYLMT: 3
QGATE	Профайл моста VM/MVS*	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QIPP	Профайл печати по сети Internet	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QIPP
QLPAUTO	Профайл автоматической установки лицензионной программы	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • INLMNU: *SIGNOFF • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG • INLPGM: QSYS/QLPINATO • DLVRY: *HOLD • SEV: 99
QLPINSTALL	Профайл установки лицензионной программы	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • DLVRY: *HOLD • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG

Таблица 150. IBM, поставляемые пользовательские профайлы (продолжение)

Имя профайла	Название	Параметры, отличающиеся от значений по умолчанию
QMGTC	Профайл Централизованного управления	<ul style="list-style-type: none"> • JOBID: QSYS/QYPSJOB
QMSF	Профайл среды почтового сервера	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QMQM	Пользовательский профайл MQSeries	<ul style="list-style-type: none"> • USRCLS: *SECADM • SPCAUT: *NONE • PRTDEV: *SYSVAL • TEXT: Пользователь MQM, являющийся владельцем библиотеки QMQM
QNFSANON	Пользовательский профайл NFS	
QNETSPLF	Профайл сетевой буферизации	
QNTP	Профайл сетевого времени	<ul style="list-style-type: none"> • JOBID: QTOTNTP • JOBID LIBRARY: QSYS
QOIUSER	Подсистема связи OSI	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS, *IOSYSCFG • CURLIB: QOSI • MSGQ: QOSI/QOIUSER • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Внутренний пользовательский профайл подсистемы связи OSI
QOSIFS	Пользовательский профайл файлового сервера OSI	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS • OUTQ: *DEV • CURLIB: *QOSIFS • CCSID: *HEX • TEXT: Внутренний пользовательский профайл файловых служб OSI
QPGMR	Профайл программиста	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹ *SAVSYS *JOBCTL • PTYLMT: 3 • ACGCDE: *BLANK
QPEX	Пользовательский профайл Индикатора статистики	<ul style="list-style-type: none"> • PTYLMT: 3 • ATNPGM: *SYSVAL • TEXT: Поставляемый IBM пользовательский профайл
QPM400	IBM Performance Management для System i (PM System i)	<ul style="list-style-type: none"> • SPCAUT: *IOSYSCFG, *JOBCTL

Таблица 150. IBM, поставляемые пользовательские профайлы (продолжение)

Имя профайла	Название	Параметры, отличающиеся от значений по умолчанию
QPRJOWN	Пользовательский профайл владельца компонентов и проектов	<ul style="list-style-type: none"> • STATUS: *DISABLED • CURLIB: QADM • TEXT: Пользовательский профайл владельца компонентов и проектов
QRDARSADM	Пользовательский профайл R/DARS	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • TEXT: Профайл администратора R/DARS
QRDAR	Профайл владельца R/DARS	<ul style="list-style-type: none"> • USRCLS: *PGMR • INLMNU: *SIGNOFF • OUTQ: *DEV • TEXT: Профайл владельца R/DARS-400
QRDARS4001	Профайл владельца R/DARS 1	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Профайл владельца R/DARS-400 1
QRDARS4002	Профайл владельца R/DARS 2	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Профайл владельца R/DARS-400 2
QRDARS4003	Профайл владельца R/DARS 3	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Профайл владельца R/DARS-400 3
QRDARS4004	Профайл владельца R/DARS 4	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Профайл владельца R/DARS-400 4
QRDARS4005	Профайл владельца R/DARS 5	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Профайл владельца R/DARS-400 5
QRMTCAL	Пользовательский профайл удаленного календаря	<ul style="list-style-type: none"> • TEXT: Пользователь удаленного календаря OfficeVision
QRJE	Профайл записи удаленного задания	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹ *SAVSYS¹ *JOBCTL
QSECOFR	Профайл системного администратора	<ul style="list-style-type: none"> • PWDEXP: *YES • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG • UID: 0 • PASSWORD: QSECOFR

Таблица 150. IBM, поставляемые пользовательские профайлы (продолжение)

Имя профайла	Название	Параметры, отличающиеся от значений по умолчанию
QSNADS	Профайл служб рассылки SNA	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QSOC	Пользовательский профайл OptiConnect	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • CURLIB: *QSOC • SPCAUT: *JOBCTL • MSGQ: QUSRSYS/QSOC
QSPL	Профайл буфера	
QSPLJOB	Профайл буферного задания	<ul style="list-style-type: none"> • AUT: *EXCLUDE
QSRV	Профайл службы	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹, *SAVSYS¹, *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Пользовательский профайл служебного агента	
QSRVBAS	Базовый профайл обслуживания	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹ *SAVSYS¹ *JOBCTL • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSVCCS	Пользовательский профайл сервера CC	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Пользовательский профайл сервера CC
QSVCM	Пользовательский профайл сервера управления клиентами	<ul style="list-style-type: none"> • TEXT: Пользовательский профайл сервера управления клиентами
QSVSM	Пользовательский профайл ECS	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • STATUS: *DISABLED • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Пользовательский профайл администратора системы SystemView
QSVSMSS	Пользовательский профайл Обслуживания управляемых систем	<ul style="list-style-type: none"> • STATUS: *DISABLED • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Пользовательский профайл Обслуживания управляемых систем
QSYS	Профайл системы	<ul style="list-style-type: none"> • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *AUDIT, *SPLCTL, *SERVICE, *IOSYSCFG

Таблица 150. IBM, поставляемые пользовательские профайлы (продолжение)

Имя профайла	Название	Параметры, отличающиеся от значений по умолчанию
QSYSOPR	Профайл системного оператора	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *ALLOBJ¹, *SAVSYS, *JOBCTL • INLMNU: SYSTEM • LIBRARY: *LIBL • MSGQ: QSYSOPR • DLVRY: *BREAK • SEV: 40
QTCM	Пользовательский профайл Triggered Cache Manager	<ul style="list-style-type: none"> • STATUS: *DISABLED
QTCP	Профайл протокола управления передачей (TCP)	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • CCSID: *HEX • SRTSEQ: *HEX
QTFTP	Упрощенный протокол передачи файлов	
QTMPLPD	Профайл поддержки печати по протоколу TCP/IP	<ul style="list-style-type: none"> • PTYLMT: 3 • AUT: *USE
QTMPLPD	Пользовательский профайл удаленного LPR	<ul style="list-style-type: none"> • JOBID: QGPL/QDFTJOBID • PWDEXPITV: *NOMAX • MSGQ: QTCP/QTMPLPD
QTMTWSG	Пользовательский профайл шлюза рабочей станции HTML	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMTWSG • TEXT: Профайл шлюза рабочей станции HTML
QTMHHTP	Пользовательский профайл шлюза рабочей станции HTML	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMHHTP • TEXT: Профайл сервера HTTP
QTMHHTP1	Пользовательский профайл шлюза рабочей станции HTML	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMHHTP • TEXT: Профайл CGI сервера HTTP
QTSTRQS	Профайл тестового запроса	
QUMB	Пользовательский профайл Ultimedia System Facility	
QUMVUSER	Пользовательский профайл Ultimedia Business Conferencing	
QUSER	Профайл пользователя рабочей станции	<ul style="list-style-type: none"> • PTYLMT: 3

Таблица 150. IBM, поставляемые пользовательские профайлы (продолжение)

Имя профайла	Название	Параметры, отличающиеся от значений по умолчанию
QX400	Пользовательский профайл файловых служб служб сообщений OSI	<ul style="list-style-type: none"> • CURLIB: *QX400 • USRCLS: *SYSOPR • MSGQ: QX400/QX400 • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Внутренний пользовательский профайл служб сообщений OSI
QYCMCIMOM	Пользовательский профайл сервера	
QYPSJSVR	Профайл сервера Централизованного управления Java	
QYPUOWN	Внутренний пользовательский профайл APU	<ul style="list-style-type: none"> • TEXT: Пользовательский профайл внутреннего APU
¹ При изменении уровня защиты системы со значения 10 или 20 на 30 или выше данное значение удаляется.		

Приложение С. Команды, поставляемые с общими правами доступа *EXCLUDE

В этом разделе приведен список команд, доступ к которым при поставке системы ограничен (т.е. установлены общие права доступа *EXCLUDE). В таблице также указано, какие поставляемые IBM пользовательские профайлы имеют права доступа к этим командам.

Дополнительная информация о пользовательских профайлах, поставляемых IBM, приведена в разделе “IBM, поставляемые пользовательские профайлы” на стр. 133.

Табл. 151 все команды, доступ к которым разрешен администратору защиты и пользователям с правами доступа *ALLOBJ, помечены символом **R** в столбце QSECOFR. Команды, доступ к которым помимо администратора защиты, есть также и у других пользовательских профайлов, поставляемых IBM, помечены символом **S** в столбце профайла, имеющего права доступа к этой команде.

Остальные команды, не перечисленные в этой таблице, являются общедоступными, т.е. вызывать их могут любые пользователи. Однако, для выполнения некоторых команд необходимы особые права доступа, например, *SERVICE или *JOBCTL. Права доступа, необходимые для запуска команд, перечислены в разделе Приложение D, “Права доступа, требуемые для объектов, используемых командами”, на стр. 359.

Если вы решили предоставить другим пользователям доступ к этим командам или задать для этих команд общие права доступа *USE, то обновите эту таблицу в соответствии с внесенными изменениями. Работа с некоторыми командами может требовать наличия доступа не только к самим командам, но и к некоторым системным объектам. Права доступа к объектам, необходимые для работы с командами, перечислены в разделе Приложение D, “Права доступа, требуемые для объектов, используемых командами”, на стр. 359.

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDCLUNODE	Ч				
ADDCMDCRQA		S	S	S	S
ADDCRGDEVE	Ч				
ADDCRGNODE	Ч				
ADDCRSDMNK	Ч				
ADDDEVDMNE	Ч				
ADDDSTQ		S	S		
ADDDSTRTE		S	S		
ADDDSTSYSN		S	S		
ADDEXITPGM	Ч				
ADDDWDFN					
ADDJWDFN					
ADDMFS	Ч				
ADDMSTPART					
ADDNETJOBE	Ч				
ADDOBJCRQA		S	S	S	S
ADDOPTCTG	Ч				

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDOPTSVR	Ч				
ADDPEXDFN		S		S	
ADDPEXFTR		S		S	
ADDPRDCRQA		S	S	S	S
ADDPTFCRQA		S	S	S	S
ADDRPYLE		S			
ADDRSCCRQA		S	S	S	S
ADDTRCFTR	Ч				
ANSQST	Ч				
ANZBESTMDL	Ч				
I ANZCMDPFR	R				
ANZDBF	Ч				
ANZDBFKEY	Ч				
ANZDFTPWD	Ч				
ANZJVM		S	S	S	S
I ANZOBJCVN	R				
ANZPFRDTA	Ч				
ANZPGM	Ч				
ANZPRB		S	S	S	S
ANZPRFACT	Ч				
ANZS34OCL	Ч				
ANZS36OCL	Ч				
APYJRNCHG		S		S	
APYPTF				S	
APYRMTPTF		S	S	S	S
CFGDSTSRV		S	S		
CFGRPDS		S	S		
CFGSYSSEC	Ч				
CHGACTSCDE	Ч				
CHGASPA	Ч				
I CHGASPACT					
CHGCLUCFG	Ч				
CHGCLUNODE	Ч				
CHGCLURCY	Ч				
CHGCLUVER	Ч				
CHGCMDCRQA		S	S	S	S
CHGCRG	Ч				
CHGCRGDEVE	Ч				
CHGCRGPRI	Ч				

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGCRSDMNK	Ч				
CHGDIRSRVA					
CHGDSTQ		S	S		
CHGDSTRTE		S	S		
CHGEXPSCDE	Ч				
CHGFCNARA	Ч				
CHGGPHFMT	Ч				
CHGGPHPKG	Ч				
CHGJOBTRC	Ч				
CHGJOBTYP	Ч				
CHGJRN		S	S	S	
CHGJRNA		S	S		
CHGLICINF	Ч				
CHGMGDSYSA		S	S	S	S
CHGMGRSRVA		S	S	S	S
CHGMSTK	Ч				
CHGNETA	Ч				
CHGNETJOBE	Ч				
CHGNFSEXP	Ч				
CHGNWSA	Ч				
CHGNWSCFG	R				
CHGOBJCRQA		S	S	S	S
CHGOPTA	Ч				
CHGPEXDFN		S		S	
CHGPRB		S	S	S	S
CHGPRDCRQA		S	S	S	S
CHGPTFCRQA		S	S	S	S
CHGPTR				S	
CHGQSTDB	Ч				
CHGRCYAP		S	S		
CHGRPYLE		S			
CHGRSCCRQA		S	S	S	S
CHGSYSLIBL	Ч				
CHGSYSVAL		S	S	S	
CHGS34LIBM	Ч				
CHKASPBAL	Ч				
CHKCMNTRC				S	
CHKMSTKVV					
CHKPRDOPT		S	S	S	S

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CLRMSTKEY					
CPHDTA	Ч				
CPYFCNARA	Ч				
CPYFRMLDIF					
CPYGPHFMT	Ч				
CPYGPHPKG	Ч				
CPYPFRCOL	R				
CPYPRDITA	Ч				
CPYPTF		S	S	S	S
CPYPTFGRP		S	S	S	S
CPYTOLDIF					
CRTADMDMN	R				
CRTAUTHLR	Ч				
CRTBESTMDL	Ч				
CRTCLS	Ч				
CRTCLU	Ч				
CRTCRG	Ч				
CRTFCNARA	Ч				
CRTGPHFMT	Ч				
CRTGHPKG	Ч				
CRTHSTDTA	Ч				
CRTJOB	Ч				
CRTNWSCFG	R				
CRTPRDITA	Ч				
CRTPFRESUM					
CRTLASREP		S			
CRTPEXDTA		S		S	
CRTQSTDB	Ч				
CRTQSTL	Ч				
CRTSBSD		S	S		
CRTUDFS	Ч				
CRTUDFS	Ч				
CRTVLDL	Ч				
CVTBASSTR	Ч				
CVTBASUNF	Ч				
CVTBGUDTA	Ч				
CVTDIR	Ч				
CVTPFRCOL	R				
CVTPFRDITA	Ч				

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CVTPFRTHD	Ч				
CVTS36FCT	Ч				
CVTS36JOB	Ч				
CVTS38JOB	Ч				
CVTTCPCPL		S	S	S	S
DB2LDIF					
DLTADMDMN	Ч				
DLTAPARDTA		S	S	S	S
DLTBESTMDL	Ч				
DLTCLU	Ч				
DLTCMNTRC				S	
DLTCRGCLU	Ч				
DLTEXSPPLF	Ч				
DLTFCNARA	Ч				
DLTGPHFMT	Ч				
DLTGPHPKG	Ч				
DLTHSTDTA	Ч				
DLTLICPGM	Ч				
DLTNWSCFG	Ч				
DLTPEXDTA		S		S	
DLTPFCOL	R				
DLTPFRDTA	Ч				
DLTPRB		S	S	S	S
DLTPTF		S	S	S	S
DLTQST	Ч				
DLTQSTDB	Ч				
DLTRMPTPF		S	S	S	S
DLTSMGOBJ		S	S	S	S
DLTUDFS	Ч				
DLTVLDL	Ч				
DLTWNTSVR	R				
DMPDLO		S	S	S	S
DMPJOB		S	S	S	S
DMPJOBINT		S	S	S	S
DMPJVM		S	S	S	S
DMPMEMINF					
DMPOBJ				S	S
DMPYSOBY		S	S	S	S
DMPTRC	Ч	S		S	

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DMPUSRPRF					
DSPDSTLOG	Ч				
DSPHSTGPH	Ч				
DSPMGDSYSA		S	S	S	S
DSPNWSCFG	Ч				
DSPPFRDTA	Ч				
DSPPFRGPH	Ч				
DSPTTF		S	S	S	S
DSPSRVSTS		S	S	S	S
EDTCPCST			S		
EDTQST	Ч				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENCCPHK	Ч				
ENCFRMMSTK	Ч				
ENCTOMSTK	Ч				
ENDASPBAL	Ч				
ENDCHTSVR	Ч				
ENDCLUNOD	Ч				
ENDCMNTRC	Ч			S	
ENDCRG	Ч				
ENDDBGSVR		S	S	S	S
ENDDW					
ENDHOSTSVR		S	S	S	S
ENDIDXMON	Ч				
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDJOBTRC	Ч				
ENDJW					
ENDMGDSYS		S	S	S	S
ENDMGRSRV		S	S	S	S
ENDMSF			S	S	S
ENDNFSSVR	Ч		S	S	S
ENDPEX		S		S	
ENDPFRTRC	Ч			S	
ENDSRVJOB		S	S	S	S
ENDSYSMGR		S	S	S	S
ENDTCP		S	S	S	S
ENDTCPNN		S	S	S	S

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ENDTCPIFC		S	S	S	S
ENDTCPSVR		S	S	S	S
ENDWCH	Ч				
GENCPHK	Ч				
GENCRSDMNK	Ч				
GENMAC	Ч				
GENPIN	Ч				
GENS36RPT	Ч				
GENS38RPT	Ч				
GRTACCAUT	Ч				
HLDCMNDEV		S	S	S	S
HLDDSTQ		S	S		
INSPTF ²				S	
INSRMTPRD		S	S	S	S
INSWNTSVR	Ч				
INZDSTQ		S	S		
INZNWSCFG	Ч				
INZSYS	Ч				
LDIF2DB					
LODOPTFMW	Ч				
LODPTF				S	
LODQSTDB	Ч				
MGRS36	Ч				
MGRS36APF	Ч				
MGRS36CBL	Ч				
MGRS36DFU	Ч				
MGRS36DSPF	Ч				
MGRS36ITM	Ч				
MGRS36LIB	Ч				
MGRS36MNU	Ч				
MGRS36MSGF	Ч				
MGRS36QRY	Ч				
MGRS36RPG	Ч				
MGRS36SEC	Ч				
MGRS38OBJ	Ч				
MIGRATE	Ч				
PKGPRDDST		S	S	S	S
PRTACTRPT	Ч				
PRTCMNTRC				S	

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
PRTCPTRPT	Ч				
PRTJOBTRPT	Ч				
PRTJOBTRC	Ч				
PRTLCKRPT	Ч				
PRTPOLRPT	Ч				
PRTRSCRPT	Ч				
PRTSYSRPT	Ч				
PRTTNSRPT	Ч				
PRTTRCRPT	Ч				
PRTDSKINF	Ч				
PRTRRLOG		S	S	S	S
PRTINTDTA		S	S	S	S
PRTPRFINT	Ч				
PWRDWN SYS	Ч		S		
RCLDBXREF	Ч				
RCLOBJOWN	Ч				
RCLOPT	Ч				
RCLSPLSTG		S	S	S	S
RCLSTG		S	S	S	S
RCLTMPSTG		S	S	S	S
RESMGRNAM	Ч	S	S	S	S
RLSCMNDEV		S	S	S	S
RLSDSTQ		S	S		
RLSIFSLCK	Ч				
RLSRMTPHS		S	S		
RMVACC	Ч				
RMVCLUNODE	Ч				
RMVCRGDEVE	Ч				
RMVCRGNODE	Ч				
RMVCRSDMNK	Ч				
RMVDEVDMNE	Ч				
RMVDFRID	R				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVDWDFN					
RMVEXITPGM	Ч				
RMVJRNCHG		S		S	
RMVJWDFN					

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RMVLANADP	Ч				
RMVMFS	Ч				
RMVNETJOBE	Ч				
RMVOPTCTG	Ч				
RMVOPTSVR	Ч				
RMVPEXDFN		S		S	
RMVPEXFTR		S		S	
RMVPTF				S	
RMVRMTPTF		S	S	S	S
RMVRPYLE		S			
RMVTRCFTR	Ч				
RSTAUT	Ч				
RST ³					
RSTCFG	Ч				
RSTDFROBJ	R				
RSTDLO	Ч				
RSTLIB	Ч				
RSTLICPGM	Ч				
RSTOBJ ³					
RSTPFRCOL	R				
RSTPFRDTA					
RSTS36F	Ч				
RSTS36FLR	Ч				
RSTS36LIBM	Ч				
RSTS38AUT	Ч				
RSTUSFCNR ⁴					
RSTUSRPRF	Ч				
RTVDSKINF	Ч				
RTVPRD		S	S	S	S
RTVPTF		S	S	S	S
RTVSMGOBJ		S	S	S	S
RUNLPDA		S	S	S	S
RUNSMGCMD		S	S	S	S
RUNSMGOBJ		S	S	S	S
RVKPUBAUT	Ч				
SAVAPARDTA		S	S	S	S
SAVLICPGM	Ч				
SAVPFRCOL	R				
SAVPFRDTA					

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
SAVRSTCHG	Ч				
SAVRSTLIB	Ч				
SAVRSTOBJ	Ч				
SBMFNCJOB	Ч				
SBMNWSCMD	Ч				
SETMSTK	Ч				
SETMSTKEY					
SNDDSTQ		S	S		
SNDPRD		S	S	S	S
SNDPTF		S	S	S	S
SNDPTFORD				S	S
SNDMSGOBJ		S	S	S	S
SNDSRVQRS				S	S
STRASPBAL	Ч				
STRBEST	Ч				
STRCHTSVR	Ч				
STRCLUNOD	Ч				
STRCMNTRC				S	
STRCRG	Ч				
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRDW					
STRHOSTSVR		S	S	S	S
STRIDXMON	Ч				
STRIPSIFC		S	S	S	S
STRJW	Ч				
STRJOBTRC					
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF ¹			S	S	S
STRNFSSVR	Ч				
STROBJCVN	R				
STRPEX		S		S	
STRPFRG	Ч				
STRPFRT	Ч				
STRPFRTRC	Ч			S	
STRRGZIDX	Ч				
STRSPLRCL	Ч				

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
STRSRVJOB		S	S	S	S
STRSST				S	
STRSYSMGR		S	S	S	S
STRS36MGR	Ч				
STRS38MGR	Ч				
STRTCP		S	S	S	S
STRTCPIFC		S	S	S	S
STRTCPsvr		S	S	S	S
STRUPDIDX	Ч				
STRWCH	Ч				
TRCASPBAL	Ч				
TRCCPIC	Ч				
TRCICF	Ч				
TRCINT		S		S	
TRCJOB		S	S	S	S
TRCTCPAPP				S	S
TRNPIN	Ч				
UPDPTFINF	Ч				
VFYCMN		S	S	S	S
VFYLNLKLPDA		S	S	S	S
VFYMSTK	Ч				
VFYPIN	Ч				
VFYPRT		S	S	S	S
VFYTAP		S	S	S	S
WRKCNTINF				S	S
WRKDEVTBL	Ч				
WRKDPCQ		S	S		
WRKDSTQ		S	S		
WRKFCNARA	Ч				
WRKJRN		S	S	S	
WRKLIB					
WRKLIBPDM					
WRKLCINF	Ч				
WRKNWSCFG	Ч				
WRKORDINF			S	S	
WRKPEXDFN		S		S	
WRKPEXFTR		S		S	
WRKPGMTBL	Ч				
WRKPRB		S	S	S	S

Таблица 151. Права доступа пользовательских профайлов, поставляемых IBM, к командам с ограниченным доступом (продолжение)

Команда	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
WRKPTFGRP		S	S	S	S
WRKPTFORD	R			S	S
WRKSRVPVD				S	S
WRKSYSACT	Ч				
WRKTRC	Ч				
WRKTXIDX	Ч				
WRKUSRTBL	Ч				
WRKWCH	Ч				
¹	Доступ к этой команде есть также у пользовательского профайла QMSF.				
²	QSRV может запускать эту команду только в том случае, если не выполняется IPL.				
³	Помимо QSYS, права доступа есть также у пользовательского профайла QRDARS400.				
⁴	Помимо QSYS, права доступа есть также у пользовательского профайла QUMB.				

Приложение D. Права доступа, требуемые для объектов, используемых командами

В таблицах этого раздела указано, какие права доступа к объектам требуются при использовании этих объектов в командах.

Например, в строке Изменить пользовательский профайл (CHGUSRPRF) таблицы перечислены все объекты, которые должны быть доступны для применения команды, а именно очередь сообщений пользователя, описание задания и начальная программа.

Таблицы упорядочены в алфавитном порядке по типу объекта. Кроме того, в приложение включены таблицы для элементов, которые не являются объектами i5/OS (задачи, буферные файлы, сетевые атрибуты и системные значения) и некоторых функций (эмуляция устройств и финансовые функции). Дополнительные замечания относительно команд приведены в сносках к таблице.

Ниже приведено описание столбцов таблиц.

Объект

В столбце *Объект* указаны объекты, права доступа к которым необходимы пользователю для применения команды.

Требуемые права доступа к объекту

В этом столбце указаны права доступа к объекту и к данным, необходимые для применения команды.

Требуемые права доступа к библиотеке

В этом столбце указаны права доступа, которые должны быть предоставлены по отношению к библиотеке, содержащей объект.

Для выполнения большинства операций необходимы права доступа *EXECUTE, которые позволяют найти объект в библиотеке. Для добавления объекта в библиотеку необходимы права доступа *READ и *ADD.

Тип объекта

Это значение относится к типу объекта, указанному в столбце Объект.

Файловая система

Это значение относится к типу файловой системы, к которой принадлежит объект.

Для интегрированной файловой системы в операционной системе i5/OS обратитесь к разделу Интегрированная файловая система.

В следующей таблице описаны права доступа, указываемые в столбце *Необходимые права доступа*. В описании приведены примеры использования этих прав доступа. В большинстве случаев для работы с объектом требуются как права доступа к объекту, так и права доступа к данным.

Таблица 152. Описание типов прав доступа

Права доступа	ФИО	Разрешенные функции
Права доступа к объекту:		

Таблица 152. Описание типов прав доступа (продолжение)

Права доступа	ФИО	Разрешенные функции
*OBJOPR	Операционные права доступа к объекту	Просмотр описания объекта. Применение объекта в тех рамках, которые определяются правами доступа пользователя к данным.
*OBJMGT	Управление объектом	Настройка параметров защиты объекта. Перемещение и переименование объекта. Все функции, допустимые для *OBJALTER и *OBJREF.
*OBJEXIST	Существование объекта	Удаление объекта. Освобождение памяти объекта. Сохранение и восстановление объекта ¹ . Изменение принадлежности объекта.
*OBJALTER	Изменение объекта	Добавление, очистка, инициализация и реорганизация элементов файла базы данных. Изменение и добавление атрибутов файлов базы данных: добавление и удаление триггеров. Изменение атрибутов пакетов SQL. Перемещение библиотеки или папки в другой ASP.
*OBJREF	Обращение к объекту	Настройка файла базы данных в качестве родительской таблицы в ограничении по ссылкам. Предположим, вам нужно определить правило, согласно которому заказ может быть добавлен в файл CUSORD только при условии, что в файле CUSMAS есть запись о заказчике. Для определения такого правила необходимо получить права доступа *OBJREF к файлу CUSMAS.
*AUTLMGT	Управление списком прав доступа	Добавление и удаление пользователей и их прав доступа в списке прав доступа.
<i>Права доступа к данным:</i>		
*READ	Чтение	Просмотр содержимого объекта, в том числе просмотр записей файла.
*ADD	Добавление	Добавление записей в объект, в том числе добавление сообщений в очередь и добавление записей в файл.
*UPD	Обновление	Изменение записей в объекте, в том числе изменение записей файла.
*DLT	Удаление	Удаление записей из объекта, в том числе удаление сообщений из очереди и записей из файла.
*EXECUTE	Выполнение	Выполнение программы, служебной программы или пакета SQL. Поиск объекта в библиотеке или каталоге.
¹ Если у пользователя есть специальные права на сохранение системы (*SAVSYS), то для сохранения и восстановления объекта права к существованию объекта не нужны.		

Кроме приведенных выше значений, в столбцах *Необходимые права доступа* могут быть указаны определенные в системе подмножества этих прав доступа. В следующей таблице описаны подмножества прав доступа к объектам и к данным.

Таблица 153. Системные права доступа

Права доступа	*ALL	*CHANGE	*USE	*EXCLUDE
<i>Права доступа к объекту</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			

Таблица 153. Системные права доступа (продолжение)

Права доступа	*ALL	*CHANGE	*USE	*EXCLUDE
*OBJALTER	X			
*OBJREF	X			
<i>Права доступа к данным</i>				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

В следующей таблице приведены дополнительные подмножества прав доступа, поддерживаемые командами CHGAUT и WRKAUT.

Таблица 154. Системные права доступа

Права доступа	*RWX	*RW	*RX	*R	*WX	*W	*X
<i>Права доступа к объекту</i>							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
<i>Права доступа к данным</i>							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Подразумеваемые права доступа, необходимые для выполнения команд

При работе с командами необходимо знать, какие применяются права доступа по умолчанию.

1. Для любой команды необходимы права доступа *USE. Эти права не указаны в таблице.
2. Для выполнения любой команды просмотра требуются операционные права доступа к поставляемому фирмой IBM файлу меню, файлу вывода на принтер или группе панелей, применяемой командой. Эти файлы и группы панелей поставляются с общими правами доступа *USE.

Общие правила относительно прав доступа к объектам, необходимых для выполнения команд

В этой таблице показаны общие правила для прав доступа к объектам, необходимых для выполнения команд

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
Изменить (CHG) с опцией F4 (Приглашение) ⁷	Текущие значения	Текущие значения будут показаны на экране, если у пользователя есть права доступа к этим значениям.	*EXECUTE
Команда, которая обращается к объекту из каталога	Каталоги, указанные в пути к объекту	*X	
	Каталог, если указан шаблон * или ?	*R	
Создание объекта в каталоге	Каталоги, указанные в пути к объекту	*X	
	Каталог, в котором будет содержаться новый объект	*WX	
Скопировать (СРУ), если целевой файл - это файл базы данных	Копируемый объект	*OBJOPR, *READ	*EXECUTE
	Команда CRTPF, если указан параметр CRTFILE (*YES)	*OBJOPR	*EXECUTE
	Целевой файл, если указан параметр CRTFILE (*YES) ¹		*ADD, *EXECUTE
	Целевой файл, если этот файл существует, и в него добавляется новый элемент	*OBJOPR, *OBJMGT, *ADD, *DLT	*ADD, *EXECUTE
	Целевой файл, если файл и элемент существуют, и указана опция *ADD	*OBJOPR, *ADD	*EXECUTE
	Целевой файл, если файл и элемент существуют, и указана опция *REPLACE	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Целевой файл, если этот файл существует, в него добавляется новый элемент, и указана опция *UPDADD. ⁸	*OBJOPR, *OBJMGT, *ADD, *UPD	*EXECUTE
	Целевой файл, если файл и элемент существуют, и указана опция *UPDADD. ⁸	*OBJOPR, *ADD, *UPD	*EXECUTE
Создать (CRT)	Создаваемый объект ²		*READ, *ADD
	Пользовательский профайл, которому будет принадлежать создаваемый объект (пользовательский профайл, запустивший задание, либо профайл группы пользователя)	*ADD	
Создать (CRT) с параметром REPLACE(*YES) ^{6,9}	Создаваемый (и заменяемый) объект ²	*OBJMGT, *OBJEXIST, *READ ⁵	*READ, *ADD
	Пользовательский профайл, которому будет принадлежать создаваемый объект (пользовательский профайл, запустивший задание, либо профайл группы пользователя)	*ADD	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
Показать (DSP) или другая операция, использующая файл вывода (OUTPUT(*OUTFILE))	Просматриваемый объект	*USE	*EXECUTE
	Файл вывода, если он не существует ³		*ADD, *EXECUTE
	Файл вывода, если он существует и в него добавляется новый элемент или если указана опция *REPLACE и элемент еще не существует	*OBJOPR, *OBJMGT или *OBJALTER, *ADD, *DLT	*ADD, *EXECUTE
	Файл вывода, если он существует и в него добавляется новый элемент или если указана опция *ADD и элемент еще не существует	*OBJOPR, *OBJMGT или *OBJALTER, *ADD	*ADD, *EXECUTE
	Файл вывода, если файл и элемент существуют, и указана опция *ADD	*OBJOPR, *ADD	*EXECUTE
	Файл вывода, если файл и элемент существуют, и указана опция *REPLACE	*OBJOPR, *OBJMGT или *OBJALTER, *ADD, *DLT	*EXECUTE
	Файл формата (QAxxxx), если файл вывода не существует	*OBJOPR	
Показать (DSP) с опцией *PRINT или Работа (WRK) с опцией *PRINT	Просматриваемый объект	*USE	*EXECUTE
	Очередь вывода ⁴	*READ	*EXECUTE
	Файл принтера (QPxxxx в QSYS)	*USE	*EXECUTE
Сохранить (SAV) или другая операция, использующая описание устройства	Описание устройства	*USE	*EXECUTE
	Файл устройства, связанный с описанием устройства, например, файл QSYSTAP для описания устройства TAP01	*USE	*EXECUTE
<p>¹ Целевой файл будет принадлежать пользователю, запустившему команду копирования, если этот пользователь не является членом группы, в профайле которого задан параметр OWNER(*GRPPRF). Если в профайле пользователя задан параметр OWNER(*GRPPRF), то владельцем целевого файла станет профайл группы. В этом случае запустившему команду пользователю должны быть предоставлены права доступа *ADD к профайлу группы, а также права на добавление элемента и на запись данных в новый файл. Для целевого файла устанавливаются такие же общие права доступа, права доступа основной группы, частные права доступа и список прав доступа, что и для исходного файла.</p> <p>² Созданный объект будет принадлежать пользователю, запустившему команду создания, если этот пользователь не является членом группы, в профайле которого указан параметр OWNER(*GRPPRF). Если в профайле пользователя задан параметр OWNER(*GRPPRF), то владельцем созданного объекта станет профайл группы. Общие права доступа к этому объекту определяются параметром AUT.</p> <p>³ Созданный файл вывода будет принадлежать пользователю, запустившему команду просмотра, если этот пользователь не является членом группы, в профайле которого указан параметр OWNER(*GRPPRF). Если в профайле пользователя задан параметр OWNER(*GRPPRF), то владельцем файла вывода станет профайл группы. Общие права доступа к файлу вывода определяются параметром CRTAUT библиотеки файла вывода.</p> <p>⁴ Если для очереди вывода задан параметр OPRCTL (*YES), то пользователю со специальными правами доступа *JOBCTL не требуются дополнительные права доступа к этой очереди. Если у пользователя есть специальные права доступа *SPLCTL, то ему не требуются никакие дополнительные права доступа к очереди вывода.</p> <p>⁵ Для файлов устройств также требуются права доступа *OBJOPR.</p>			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
6	В среде S/38 параметр REPLACE недоступен. Вместо добавления параметра REPLACE(*YES) нажмите в меню программиста функциональную клавишу, предназначенную для удаления текущего объекта.		
7	Также необходимы права на выполнение соответствующей команды (DSP).		
8	Опция *UPDADD доступна только в параметре MBROPT команды CPYF.		
9	Это не относится к параметру REPLACE команды CRTJVAPGM.		

Общие команды для большинства объектов

В этой таблице перечислены команды в алфавитном порядке, применимые для большинства объектов.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Таблица 155. Общие команды для большинства объектов

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ALCOBJ ^{1,2,11}	Объект	*OBJOPR	*EXECUTE
ANZOBJCVN (Q) ²⁰			
ANZUSROBJ ²⁰			
CHGOBJAUD ¹⁸	ASP (если он указан)	*USE	
CHGOBJD ³	Объект, если это файл	*OBJOPR, *OBJMGT	*EXECUTE
	Объект, если это не файл	*OBJMGT	*EXECUTE
CHGOBJOWN ^{3,4}	Объект	*OBJEXIST	*EXECUTE
	Объект (если это файл, библиотека, описание подсистемы)	*OBJOPR, *OBJEXIST	*EXECUTE
	Объект (если указано *AUTL)	Права владельца или *ALLOBJ	*EXECUTE
	Прежний пользовательский профайл	*DLT	*EXECUTE
	Новый пользовательский профайл	*ADD	*EXECUTE
	ASP (если он указан)	*USE	
CHGOBJPGP ³	Объект	*OBJEXIST	*EXECUTE
	Объект (если это файл, библиотека, описание подсистемы)	*OBJOPR, *OBJEXIST	*EXECUTE
	Объект (если указано *AUTL)	Права владельца и *OBJEXIST, либо *ALLOBJ	*EXECUTE
	Прежний пользовательский профайл	*DLT	
	Новый пользовательский профайл	*ADD	
	ASP (если он указан)	*USE	
CHKOBJ ³	Объект	Права доступа, указанные в параметре AUT ¹⁴	*EXECUTE

Таблица 155. Общие команды для большинства объектов (продолжение)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CPROBJ	Объект	*OBJMGT	*EXECUTE
CHKOBJTG ¹¹ (Q)			
CRTDUPOBJ ^{3,9,11,21}	Новый объект		*USE, *ADD
	Копируемый объект, если это *AUTL	*AUTLMGT	*USE, *ADD
	Копируемый объект любого другого типа	*OBJMGT, *USE	*USE
	Команда CRTSAVF (если объект - файл сохранения)	*OBJOPR	
	ASP (если он указан)	*USE	
DCPROBJ	Объект	*USE	*EXECUTE
DLCOBJ ^{1,11}	Объект	*OBJOPR	*EXECUTE
DMPOBJ (Q) ³	Объект	*OBJOPR, *READ	*EXECUTE
DMPSYSOBJ (Q)	Объект	*OBJOPR, *READ	*EXECUTE
DSPOBJAUT ³	Объект (для просмотра информации обо всех правах доступа)	Специальные права *OBJMGT или *ALLOBJ или права владельца	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
	ASP (если он указан)	*USE	
DSPOBJD ^{2, 28}	Файл вывода	См. общие правила.	См. общие правила.
	Права доступа	Любые права доступа, отличные от *EXCLUDE	*EXECUTE
	ASP (если он указан)	*EXECUTE	
EDTOBJAUT ^{3,5,6,15}	Объект	*OBJMGT	*EXECUTE
	Объект (если это файл)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, если объект защищен списком прав доступа	Любые, кроме *EXCLUDE	
	ASP (если он указан)	*USE	
GRTOBJAUT ^{3,5,6,15}	Объект	*OBJMGT	*EXECUTE
	Объект (если это файл)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, если объект защищен списком прав доступа	Любые, кроме *EXCLUDE	
	ASP (если он указан)	*USE	
	Модельный ASP (если он указан)	*EXECUTE	
	Модельный объект	*OBJMGT или права владельца	*EXECUTE

Таблица 155. Общие команды для большинства объектов (продолжение)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
MOV OBJ ^{3,7,12}	Объект	*OBJMGT	
	Объект (если указано *FILE)	*ADD, *DLT, *EXECUTE	
	Объект (не *FILE),	*DLT, *EXECUTE	
	Исходная библиотека		*CHANGE
	Целевая библиотека		*READ, *ADD
	ASP (если он указан)	*USE	
PRTADPOBJ ^{26(Q)}			
PRTPUBAUT ²⁶			
PRTUSROBJ ²⁶			
PRTPVTAUT ²⁶			
RCLDBXREF			
RCLOBJOWN (Q)			
RCLSTG (Q)			
RCLTMPSTG (Q)	Объект	*OBJMGT	*EXECUTE
RMVDFRID (Q) ¹⁰			
RNMOBJ ^{3,11}	Объект	*OBJMGT	*UPD, *EXECUTE
	Объект, если *AUTL	*AUTLMGT	*EXECUTE
	Объект (если указано *FILE)	*OBJOPR, *OBJMGT	*UPD, *EXECUTE
	ASP (если он указан)	*USE	
RSTDFROBJ (Q) ¹⁰	Вывод на принтер QSYS/QPSRLDSP, если задано OUTPUT(*PRINT)	*USE	*EXECUTE
	Файл вывода, если он указан	См. общие правила	См. общие правила
	Файл описания полей QSYS/QASRRSTO, если указан несуществующий файл вывода	*USE	*EXECUTE
RSTOBJ (Q) ^{3,13, 31, 33}	Объект, если он уже существует в библиотеке	*OBJEXIST ⁸	*EXECUTE, *ADD
	Объект, если он относится к типу *CFGL, *CNL, *CTLD, *DEVD, *LIND или *NWID	*CHANGE и *OBJMGT	*EXECUTE
	Определение носителя	*USE	*EXECUTE
	Очереди сообщений, восстанавливаемые в библиотеке, в которой они уже существуют	*OBJOPR, *OBJEXIST ⁸	*EXECUTE, *ADD
	Пользовательский профайл, которому принадлежат создаваемые объекты	*ADD ⁸	
	Программа, принимающая права доступа	Права владельца, либо *SECADM и *ALLOBJ	*EXECUTE
	Целевая библиотека	*EXECUTE, *ADD ⁸	
	Библиотека сохраняемого объекта, если указан параметр VOL(*SAVVOL)	*USE ⁸	
	Файл сохранения	*USE	*EXECUTE

Таблица 155. Общие команды для большинства объектов (продолжение)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RSTOBJ (Q)	Лентопротяжное устройство или оптический накопитель	*USE	*EXECUTE
	Файл магнитной ленты (QSYSTAP) или дискеты (QSYSDKT)	*USE ⁸	*EXECUTE
	Оптический файл (OPTFILE) ²²	*R	Не применимо
	Родительский каталог файла OPTFILE ²²	*X	Не применимо
	Префикс пути к файлу OPTFILE ²²	*X	Не применимо
	Оптический том ²⁴	*USE	Не применимо
	Вывод на принтер QSYS/QPSRLDSP, если задано OUTPUT(*PRINT)	*USE	*EXECUTE
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Файл описания полей QSYS/QASRRSTO, если указан несуществующий файл вывода	*USE	*EXECUTE
Описание ASP ²⁵	*USE		
RSTSYSINF	Файл сохранения	*USE	*EXECUTE
	Лентопротяжное устройство или оптический накопитель	*USE	*EXECUTE
	Оптический файл (OPTFILE) ²²	*R	Не применимо
	Родительский каталог файла OPTFILE ²²	*X	Не применимо
	Префикс пути к файлу OPTFILE ²²	*X	Не применимо
	Оптический том ²⁴	*USE	Не применимо
RVKPUBAUT ²⁰			
RTVOBJD ^{2, 29}	Объект	Любые права доступа, отличные от *EXCLUDE	*EXECUTE
RVKOBJAUT ^{3,5,15, 27}	ASP (если он указан)	*USE	
SAVCHGOBJ ^{3, 32}	Объект (8)	*OBJEXIST	*EXECUTE
	Лентопротяжное устройство или оптический накопитель	*USE	*EXECUTE
	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE
	Файл сохранения (если в нем есть записи)	*OBJMGT, *USE, *ADD	*EXECUTE
	Очередь сообщений о сохранении активных объектов	*OBJOPR, *ADD	*EXECUTE
	Пространство пользователя команды, если задано	*USE	*EXECUTE

Таблица 155. Общие команды для большинства объектов (продолжение)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
SAVCHGOBJ	Оптический файл (OPTFILE) ²²	*RW	Не применимо
	Родительский каталог файла OPTFILE ²²	*WX	Не применимо
	Префикс пути к оптическому файлу (OPTFILE) ²²	*X	Не применимо
	Корневой каталог (/) оптического тома ^{22, 23}	*RWX	Не применимо
	Оптический том ²⁴	*CHANGE	
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Файл описания полей QSYS/QASAVOBJ, если указан несуществующий файл вывода	*USE ⁸	*EXECUTE
	Вывод на принтер QSYS/QPSAVOBJ	*USE ⁸	*EXECUTE
	Описание ASP ²⁵	*USE	
SAVOBJ ^{3, 32}	Объект	*OBJEXIST ⁸	*EXECUTE
	Определение носителя	*USE	*EXECUTE
	Лентопротяжное устройство или оптический накопитель	*USE	*EXECUTE
	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE
	Файл сохранения (если в нем есть записи)	*OBJMGT, *USE, *ADD	*EXECUTE
	Очередь сообщений о сохранении активных объектов	*OBJOPR, *ADD	*EXECUTE
	Пространство пользователя команды, если задано	*USE	*EXECUTE
SAVOBJ	Оптический файл (OPTFILE) ²²	*RW	Не применимо
	Родительский каталог файла OPTFILE ²²	*WX	Не применимо
	Префикс пути к файлу OPTFILE ²²	*X	Не применимо
	Корневой каталог (/) оптического тома ^{22, 23}	*RWX	Не применимо
	Оптический том ²⁴	*CHANGE	
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Файл описания полей QSYS/QASAVOBJ, если указан несуществующий файл вывода	*USE ⁸	*EXECUTE
	Вывод на принтер QSYS/QPSAVOBJ	*USE ⁸	*EXECUTE
	Описание ASP ²⁵	*USE	
SAVSTG ¹⁰			
SAVSYS ¹⁰	Лентопротяжное устройство, оптический накопитель	*USE	*EXECUTE
	Корневой каталог (/) оптического тома ²²	*RWX	Не применимо
	Оптический том ²⁴	*CHANGE	Не применимо

Таблица 155. Общие команды для большинства объектов (продолжение)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
SAVSYINF	Определение носителя	*USE	*EXECUTE
	Лентопротяжное устройство или оптический накопитель	*USE	*EXECUTE
	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE
	Файл сохранения (если в нем есть записи)	*OBJMGT, *USE, *ADD	*EXECUTE
	Оптический файл (OPTFILE) ²²	*RW	Не применимо
	Родительский каталог файла OPTFILE ²²	*WX	Не применимо
	Префикс пути к файлу OPTFILE ²²	*X	Не применимо
	Корневой каталог (/) оптического тома ^{22, 23}	*RWX	Не применимо
	Оптический том ²⁴	*CHANGE	
SAVRSTCHG	В исходной системе - те же права доступа, что и для команды SAVCHGOBJ.		
	В целевой системе - те же права доступа, что и для команды RSTOBJ.		
	Описание ASP ²⁵	*USE	
SAVRSTOBJ	В исходной системе - те же права доступа, что и для команды SAVOBJ.		
	В целевой системе - те же права доступа, что и для команды RSTOBJ.		
	Описание ASP ²⁵	*USE	
SETOBJACC	Объект	*OBJOPR	*EXECUTE
STROBJCVN (Q) ²⁰			
STRSAVSYNC ³⁴			
WRKOBJ ¹⁹	Объект	Любые права доступа	*USE
WRKOBJLCK	Объект		*EXECUTE
	ASP	*EXECUTE	
WRKOBJOWN ¹⁷	Пользовательский профайл	*READ	*EXECUTE
WRKOBJPGP ¹⁷	Пользовательский профайл	*READ	*EXECUTE
WRKOBJPVT ¹⁷	Пользовательский профайл	*READ	*EXECUTE
¹	Список типов объектов, которые можно захватывать и освобождать, приведен в описании ключевого слова OBJTYPE команды ALCOBJ.		
²	Необходимы любые права доступа к объекту, отличные от *EXCLUDE.		
³	Эта команда неприменима к документам и папкам. Воспользуйтесь соответствующей командой для объекта библиотеки документов (DLO).		
⁴	Для изменения владельца программы, служебной программы или пакета SQL, принимающих права доступа, необходимы специальные права доступа *ALLOBJ и *SECADM.		
⁵	Вы должны быть владельцем объекта, либо у вас должны быть права доступа *OBJMGT, а также предоставляемые или аннулируемые права доступа.		

Таблица 155. Общие команды для большинства объектов (продолжение)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
6	Для того чтобы вы могли предоставить права доступа *OBJMGT или *AUTLMGT, вы должны быть владельцем, либо у вас должны быть права доступа *ALLOBJ.		
7	Эта команда неприменима к пользовательским профайлам, описаниям контроллеров, устройств и линий связи, документам, библиотекам документов и папкам.		
8	Если пользователю предоставлены специальные права доступа *SAVSYS, то указанные права доступа не нужны.		
9	Если в профайле пользователя, запустившего команду CRTDUPOBJ, задан параметр OWNER(*GRPPRF), то владельцем нового объекта станет профайл группы. При копировании прав доступа в новый объект, принадлежащий профайлу группы, действуют следующие ограничения: <ul style="list-style-type: none"> • У пользователя, выполняющего команду, должны быть права доступа к копируемому объекту. Права доступа можно получить из принятых прав доступа или посредством профайла группы. • Если при копировании прав доступа в новый объект возникает ошибка, то создаваемый объект удаляется. 		
10	Необходимы специальные права доступа *SAVSYS.		
11	Эта команда неприменима к журналам и получателям журналов.		
12	Эта команда неприменима к журналам и получателям журналов, за исключением случаев, когда исходная библиотека - QRCL, а целевая библиотека - это начальная библиотека журнала или получателя журнала.		
13	Для того чтобы присвоить параметру Разрешить различия в объектах (ALWOBJDIF) значение, отличное от *NONE, необходимы специальные права доступа *ALLOBJ.		
14	Для проверки предоставленных пользователю прав доступа к объекту вам должны быть предоставлены все проверяемые права доступа. Например, для того чтобы проверить, есть ли у пользователя права доступа *OBJEXIST к файлу FILEB, необходимы права доступа *OBJEXIST к файлу FILEB.		
15	Для того чтобы связать объект со списком прав доступа или аннулировать такую связь, необходимы любые из следующих прав доступа: <ul style="list-style-type: none"> • Права владельца объекта. • Права доступа *ALL к объекту. • Специальные права доступа *ALLOBJ. 		
16	Если с исходным или переименованным файлом связан владелец прав доступа, то необходимы права доступа *ALL к этому владельцу.		
17	Эта команда не поддерживает файловую систему QOPT.		
18	Необходимы специальные права доступа *AUDIT.		
19	Для выполнения отдельной операции нужны права доступа, запрашиваемые этой операцией.		
20	Необходимы специальные права доступа *ALLOBJ.		

Таблица 155. Общие команды для большинства объектов (продолжение)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
21	Все права доступа к исходному объекту копируются в новый объект. Основная группа нового объекта определяется исходя из типа прав доступа группы (GRPAUTTYR), заданного в профайле пользователя, запустившего команду. Если для исходного объекта задана основная группа, то не требуется, чтобы с новым объектом была связана та же основная группа. Однако все права доступа основной группы к исходному объекту будут продублированы для нового объекта.		
22	Наличие этих прав доступа проверяется только для оптических носителей формата UDF.		
23	Эти права доступа проверяются только при очистке оптического тома.		
24	Оптические тома фактически не являются объектами системы. Связь между оптическим томом и списком прав доступа, применяемым для ограничения доступа к тому, устанавливается функцией поддержки оптической памяти.		
25	Права доступа необходимы только в том случае, если для выполнения сохранения или восстановления необходимо изменить пространство имен библиотек.		
26	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ или *AUDIT.		
27	*** Угроза защите *** Аннулирование всех прав доступа, специально предоставленных пользователю по отношению к некоторому объекту, может привести к тому, что у пользователя будет больше прав доступа, чем до аннулирования. Если у пользователя есть права доступа *USE к объекту и права доступа *CHANGE к списку прав доступа, защищающему объект, то в случае аннулирования прав доступа *USE у пользователя будут права доступа *CHANGE к объекту.		
28	Для просмотра значения контроля текущего объекта необходимы специальные права доступа *ALLOBJ или *AUDIT. В противном случае будет показано значение *NOTAVL, указывающее, что значение недоступно для просмотра.		
29	Для извлечения значения контроля текущего объекта необходимы специальные права доступа *ALLOBJ или *AUDIT. В противном случае будет возвращено значение *NOTAVL, указывающее, что значения недоступны для извлечения.		
30	Права доступа, необходимые для преобразования программ, служебных программ и модулей, указаны в описаниях команд CHGPGM, CHGSRVPGM и CHGMOD.		
31	Для указания в параметре PVTAUT значения *YES необходимы специальные права доступа *ALLOBJ.		
32	Для указания в параметре PVTAUT значения *YES необходимы специальные права доступа *ALLOBJ или *SAVSYS.		
33	Для указания имени параметра DFRID необходимы специальные права доступа *SAVSYS.		
34	Необходимы специальные права доступа *SAVSYS и *JOBCTL.		

Команды восстановления путей доступа

В этой таблице перечислены права доступа, необходимые для выполнения команд восстановления путей доступа

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGRCYAP ¹ (Q)	ASP (если он указан)	*USE	
DSPRCYAP ¹	ASP (если он указан)	*USE	
EDTRBDAP ² (Q)			
EDTRCYAP ¹ (Q)	ASP (если он указан)	*USE	
¹ Для выполнения этой команды необходимы специальные права доступа *JOBCTL. ² Для выполнения этой команды необходимы специальные права доступа *ALLOBJ.			

Команды Advanced Function Presentation (AFP)

В этой таблице перечислены права доступа, необходимые для выполнения команд Advanced Function Presentation (AFP).

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDFNTBLE	Таблица шрифтов DBCS	*CHANGE	*EXECUTE
CHGCDEFNT	Ресурс шрифта	*CHANGE	*EXECUTE
CHGFNTBLE	Таблица шрифтов DBCS	*CHANGE	*EXECUTE
CRTFNTRSC	Исходный файл	*USE	*EXECUTE
	Ресурс шрифта: REPLACE(*NO)		*READ, *ADD
	Ресурс шрифта: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTFNNTBL	Таблица шрифтов DBCS		*READ, *ADD
CRTFORMDF	Исходный файл	*USE	*EXECUTE
	Определение формы: REPLACE(*NO)		*READ, *ADD
	Определение формы: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTOVL	Исходный файл	*USE	*EXECUTE
	Перекрытие: REPLACE(*NO)		*READ, *ADD
	Перекрытие: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTPAGDFN	Исходный файл	*USE	*EXECUTE
	Описание страницы: REPLACE(*NO)		*READ, *ADD
	Описание страницы: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTPAGSEG	Исходный файл	*USE	*EXECUTE
	Сегмент страницы: REPLACE(*NO)		*READ, *ADD
	Сегмент страницы: REPLACE(*YES)	См. общие правила.	*READ, *ADD
DLTFNTRSC	Ресурс шрифта	*OBJEXIST	*EXECUTE
DLTFNNTBL	Таблица шрифтов DBCS	*CHANGE	*EXECUTE
DLTFORMDF	Определение формы	*OBJEXIST	*EXECUTE
DLTOVL	Перекрытие	*OBJEXIST	*EXECUTE
DLTPAGDFN	Определение страницы	*OBJEXIST	*EXECUTE
DLTPAGSEG	Сегмент страницы	*OBJEXIST	*EXECUTE
DSPCDEFNT	Ресурс шрифта	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DSPFNTRSCA	Ресурс шрифта	*USE	*EXECUTE
DSPFNTTBL	Таблица шрифтов DBCS	*USE	*EXECUTE
RMVFNTTBLE	Таблица шрифтов DBCS	*CHANGE	*EXECUTE
WRKFNTRSC ¹	Ресурс шрифта	*USE	*USE
WRKFORMDF ¹	Определение формы	*USE	*USE
WRKOVL ¹	Перекрытие	*USE	*USE
WRKPAGDFN ¹	Определение страницы	Любые права доступа	*USE
WRKPAGSEG ¹	Сегмент страницы	*USE	Любые права доступа
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.			

Команды для работы с сокетами AF_INET для SNA

В этой таблице перечислены права доступа, необходимые для выполнения команды для работы с сокетами AF_INET для SNA.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам:

Для выполнения следующих команд не требуются никакие права доступа к объектам:			
ADDIPSIFC ¹ ADDIPS RTE ¹ ADDIPSLOC ¹ CFGIPS	CHGIPSIFC ¹ CHGIPSLOC ¹ CHGIPSTOS ¹ CVTIPSIFC	CVTIPSLOC ENDIPSIFC (Q) PRTIPSCFG RMVIPSIFC ¹	RMVIPSLOC ¹ RMVIPS RTE ¹ STRIPSIFC (Q)
¹ Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			

Команды предупреждений

В этой таблице перечислены права доступа, необходимые для выполнения команд предупреждений.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDALRD	Таблица предупреждений	*USE, *ADD	*EXECUTE
CHGALRD	Таблица предупреждений	*USE, *UPD	*EXECUTE
CHGALRTBL (Q)	Таблица предупреждений	*CHANGE	*EXECUTE
CRTALRTBL (Q)	Таблица предупреждений		*READ, *ADD
DLTALR	Физический файл QAALERT	*USE, *DLT	*EXECUTE
DLTALRTBL (Q)	Таблица предупреждений	*OBJEXIST	*EXECUTE
RMVALRD	Таблица предупреждений	*USE, *DLT	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
WRKALR ¹	Физический файл QAALERT	*USE	*EXECUTE
WRKALRD ¹	Таблица предупреждений	*USE	*EXECUTE
WRKALRTBL ¹	Таблица предупреждений	*READ	*USE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.			

команды для разработки приложений

В этой таблице перечислены права доступа, необходимые для выполнения команд разработки приложений.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
FNDSTRPDM	Часть исходного кода	*READ	*EXECUTE
MRGFORMD	Описание формы	*READ	*EXECUTE
STRAPF ¹	Исходный файл	*OBJMGT, *CHANGE	*READ, *ADD
	Команды CRTPF, CRTLF, ADDPFM, ADDLFM и RMVM	*USE	*EXECUTE
STRBGU ¹	Диаграмма	*OBJMGT, *CHANGE	*EXECUTE
STRDFU ¹	Программа (если выбрана опция создания программы)		*READ, *ADD
	Программа (если выбрана опция изменения или удаления программы)	*OBJEXIST	*EXECUTE
	Программа (если выбрана опция изменения или просмотра данных)	*USE	*EXECUTE
	Файл базы данных (если выбрана опция изменения данных)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Файл базы данных (если выбрана опция просмотра данных)	*USE	*EXECUTE
	Файл дисплея (если выбрана опция просмотра или изменения данных)	*USE	*EXECUTE
	Файл дисплея (если выбрана опция изменения программы)	*USE	*EXECUTE
	Файл дисплея (если выбрана опция удаления программы)	*OBJEXIST	*EXECUTE
STRPDM ¹			
STRRLU	Исходный файл	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Редактировать, добавить или изменить элемент	*OBJOPR, *OBJMGT	*READ, *ADD
	Найти элемент	*OBJOPR	*EXECUTE
	Напечатать прототип отчета	*OBJOPR	*EXECUTE
	Удалить элемент	*OBJOPR, *OBJEXIST	*EXECUTE
	Изменить тип или описание элемента	*OBJOPR	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRSDA	Исходный файл	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Обновить и добавить новый элемент	*CHANGE, *OBJMGT	*READ, *ADD
	Удалить элемент	*ALL	*EXECUTE
STRSEU ¹	Исходный файл	*USE	*EXECUTE
	Редактировать или изменить элемент	*CHANGE, *OBJMGT	*EXECUTE
	Добавить элемент	*USE, *OBJMGT	*READ, *ADD
	Найти элемент	*USE	*EXECUTE
	Распечатать элемент	*USE	*EXECUTE
	Удалить элемент	*USE, *OBJEXIST	*EXECUTE
	Изменить тип или описание элемента	*USE, *OBJMGT	*EXECUTE
WRKLIBPDM ^{1,4}			
WRKMBRPDM ¹	Исходный файл	*USE	*EXECUTE
WRKOBJPDM ¹	Файл	*READ или права владельца	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией. ² Группа соответствует библиотеке. ³ Проект состоит из одной или нескольких групп (библиотек). ⁴ Для применения этой команды необходимы специальные права доступа *ALLOBJ.			

Команды для работы с владельцами прав доступа

В этой таблице перечислены права доступа, необходимые для выполнения команд с владельцами прав доступа.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTAUTHLR (Q)	Связанный объект (если существует)	*ALL	*EXECUTE
DLTAUTHLR	Владелец прав доступа	*ALL	*EXECUTE
DSPAUTHLR	Файл вывода	См. общие правила.	См. общие правила.

Команды списка прав доступа

В этой таблице перечислены права доступа, необходимые для выполнения команд списка прав доступа.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке QSYS
ADDAUTLE ¹	*AUTL	*AUTLMGT или права владельца	*EXECUTE
CHGAUTLE ¹	*AUTL	*AUTLMGT или права владельца	*EXECUTE
CRTAUTL			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке QSYS
DLTAUTL	*AUTL	Права владельца или *ALLOBJ	*EXECUTE
DSPAUTL	*AUTL		*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
DSPAUTLDLO	*AUTL	*USE	*EXECUTE
DSPAUTLOBJ	*AUTL	*READ	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
EDTAUTL ¹	*AUTL	*AUTLMGT или права владельца	*EXECUTE
RMVAUTLE ¹	*AUTL	*AUTLMGT или права владельца	*EXECUTE
RTVAUTLE ²	*AUTL	*AUTLMGT или права владельца	*EXECUTE
WRKAUTL ^{3,4,5}	*AUTL		
¹	Вы должны быть владельцем объекта или иметь права на управление списками прав доступа.		
²	Если у вас нет прав доступа *OBJMGT или *AUTLMGT, то вы можете получить записи о своих правах доступа и правах доступа *PUBLIC. Для получения собственных прав доступа необходимы права на чтение (*READ) своего профайла.		
³	Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.		
⁴	Вы не должны быть исключены (*EXCLUDE) из списка прав доступа.		
⁵	Требуются какие-либо права доступа к списку прав доступа.		

Команды для работы с каталогами связывания

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с каталогом связывания.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDBNDDIRE	Каталог связывания	*OBJOPR, *ADD	*USE
CRTBNDDIR	Каталог связывания		*READ, *ADD
DLTBNDDIR	Каталог связывания	*OBJEXIST	*EXECUTE
DSPBNDDIR	Каталог связывания	*READ, *OBJOPR	*USE
RMVBNDDIRE	Каталог связывания	*OBJOPR, *DLT	*READ, *OBJOPR
WRKBNDDIR ¹	Каталог связывания	Любые права доступа	*USE
WRKBNDDIRE ¹	Каталог связывания	*READ, *OBJOPR	*USE
¹	Для выполнения отдельной операции нужны права доступа, запрашиваемые этой операцией.		

Команды для работы с описанием запроса на изменение

В этой таблице перечислены права доступа, необходимые для выполнения команд описания запроса на изменение.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDCMDCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
ADDOBJCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
ADDPRDCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
ADDPTFCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
ADDRSCCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
CHGCMDCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
CHGOBJCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
CHGPRDCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
CHGPTFCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
CHGCRQD	описание запроса на изменение	*CHANGE	*EXECUTE
CHGRSCCRQA (Q)	Описание запроса на изменение	*CHANGE	*EXECUTE
CRTCRQD	Описание запроса на изменение		*READ, *ADD
DLTCRQD	Описание запроса на изменение	*OBJEXIST	*EXECUTE
RMVCRQDA	Описание запроса на изменение	*CHANGE	*EXECUTE
WRKCRQD ¹	Описание запроса на изменение		*EXECUTE

¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.

Команды для работы с диаграммами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с диаграммами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTCHTFMT	Формат диаграммы	*OBJEXIST	*EXECUTE
DSPCHT	Формат диаграммы	*USE	*USE
	Файл базы данных	*USE	*USE
DSPGDF	Файл базы данных	*USE	*USE
STRBGU (опция 3) ²	Формат диаграммы	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT ¹	Формат диаграммы	Любые права доступа	*USE

¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.

² Опция 3 меню BGU, которое появляется при запуске STRGBU, - это функция Изменить формат диаграммы.

Команды для работы с классами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с классами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGCLS	Класс	*OBJMGT, *OBJOPR	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTCLS	Класс		*READ, *ADD
DLTCLS	Класс	*OBJEXIST	*EXECUTE
DSPCLS	Класс	*USE	*EXECUTE
WRKCLS ¹	Класс	*OBJOPR	*USE
¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.			

Команды для работы с классом обслуживания

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с классом обслуживания.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGCOSD ³	Описание класса обслуживания	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD ³	Описание класса обслуживания		
DLTCOSD	Описание класса обслуживания	*OBJEXIST	*EXECUTE
DSPCOSD	Описание класса обслуживания	*USE	*EXECUTE
WRKOSD ^{1,2}	Описание класса обслуживания	*OBJOPR	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.			
² Требуется какие-либо права доступа к объекту.			
³ Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			

Команды для работы с кластерами

В этой таблице перечислены права доступа, необходимые для выполнения команд с кластерами.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставить права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDCLUNODE (Q) ¹	Служебная программа QCSTCTL	*USE	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDCRGDEVE (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
	Описание сетевого сервера	*USE, *OBJMGT	
ADDCRGNODE (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Очередь сообщений о передаче управления	*OBJOPR, *ADD	*EXECUTE
	Пользовательская очередь рассылки информации	*OBJOPR, *ADD	*EXECUTE
ADDDEVDMNE (Q) ¹	Служебная программа QCSTDD	*USE	
CHGCLUCFG (Q) ¹	Служебная программа QCSTCTL2	*USE	
CHGCLUNODE (Q) ¹	Служебная программа QCSTCTL	*USE	
CHGCLURCY	Группа ресурсов кластера	*USE	
		*JOBCTL	
		*SERVICE или функция Служебная трассировка	
CHGCLUVER (Q) ¹	Служебная программа QCSTCTL2	*USE	
CHGCRG (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Очередь сообщений о передаче управления	*OBJOPR, *ADD	*EXECUTE
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
Описание сетевого сервера	*USE, *OBJMGT		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGCRGDEVE (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
	Описание сетевого сервера	*USE, *OBJMGT	
CHGCRGPRI (Q) ¹	Служебная программа QCSTCRG2	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Команда Включить/Выключить конфигурацию (VFYCFG)	*USE	
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
	Описание сетевого сервера	*USE, *OBJMGT	
CRTADMDMN (Q) ^{1, 3}	Пользовательский профайл QCLUSTER	*USE	
CRTCLU (Q) ¹	Служебная программа QCSTCTL	*USE	
CRTCRG (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Библиотека группы ресурсов кластера		*OBJOPR, *ADD, *READ (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Пользовательская очередь рассылки информации	*OBJOPR, *ADD	*EXECUTE
	Очередь сообщений о передаче управления	*OBJOPR, *ADD	*EXECUTE
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
	Описание сетевого сервера	*USE, *OBJMGT	
DLTADMDMN (Q) ¹	Группа ресурсов кластера	*OBJEXIST, *USE	
	QUSRSYS	*EXECUTE	
	QCLUSTER	*USE	
DLTCLU (Q) ¹	Служебная программа QCSTCTL	*USE	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTCRG ¹	Группа ресурсов кластера	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
DLTCRGCLU (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Группа ресурсов кластера	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
DMPCLUTRC	Группа ресурсов кластера	*USE	
		*SERVICE или функция Служебная трассировка	
DSPCLUINF			
DSPCRGINF	Группа ресурсов кластера	*USE	*EXECUTE (QUSRSYS)
ENDCLUNOD (Q) ¹	Служебная программа QCSTCTL	*USE	
ENDCHTSVR (Q)	Список прав доступа	*CHANGE	
ENDCRG (Q) ¹	Служебная программа QCSTCRG2	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE (QUSRSYS)
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
RMVCLUNODE (Q) ¹	Служебная программа QCSTCTL	*USE	
RMVCRGDEVE (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
	Описание сетевого сервера	*USE, *OBJMGT	
RMVCRGNODE (Q) ¹	Служебная программа QCSTCRG1	*USE	
	Группа ресурсов кластера	*CHANGE, *OBJEXIST	*EXECUTE
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
	Описание сетевого сервера	*USE, *OBJMGT	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RMVDEVDMNE (Q) ¹	Служебная программа QCSTDD	*USE	
STRCHTSVR	Список прав доступа	*CHANGE	
STRCLUNOD (Q) ¹	Служебная программа QCSTCTL	*USE	
STRCRG (Q) ¹	Служебная программа QCSTCRG2	*USE	
	Группа ресурсов кластера	*CHANGE	*EXECUTE
	Программа выхода	*EXECUTE ²	*EXECUTE ²
	Пользовательский профайл для выполнения программы выхода	*USE	
	Описание устройства	*USE, *OBJMGT	
	Описание контроллера	*USE, *OBJMGT	
	Описание линии	*USE, *OBJMGT	
	Описание сетевого сервера	*USE, *OBJMGT	
WRKCLU ⁴	Группа ресурсов кластера	*USE	*EXECUTE
¹	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.		
²	Права доступа применяются к вызывающему пользовательскому профайлу и к пользовательскому профайлу, предназначенному для выполнения программы выхода.		
³	Вызывающему пользовательскому профайлу предоставляются права доступа *CHANGE и *OBJEXIST к группе ресурсов кластера.		
⁴	У вас должны быть специальные права доступа *SERVICE или права доступа к функции i5/OS Служебная трассировка, предоставленные с помощью функции Администрирование приложений Навигатора System i. Список пользователей, которым разрешено выполнять операции трассировки, также можно изменить с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав ИД функции QIBM_SERVICE_TRACE.		

Команды для работы с командами (*CMD)

В этой таблице перечислены права доступа, необходимые для команд, выполняемых над командами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGCMD	Команда	*OBJMGT	*EXECUTE
CHGCMDDDFT	Команда	*OBJMGT, *USE	*EXECUTE
CHGPRXCMD	Команда проху	*OBJMGT	*EXECUTE
CRTCMD	Исходный файл	*USE	*EXECUTE
	Команда: REPLACE(*NO)		*READ, *ADD
	Команда: REPLACE(*YES)	См. общие правила.	См. общие правила.
CRTPRXCMD	Команда проху: REPLACE(*NO)		*READ, *ADD
	Команда проху: REPLACE(*YES)	См. общие правила на стр. D-2	См. общие правила на стр. D-2
DLTCMD	Команда	*OBJEXIST	*EXECUTE
DSPCMD	Команда	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
GENCMDDOC ³	Команда	*USE	*EXECUTE
	Группа панелей (связанная)	*USE	*EXECUTE
	Файл вывода: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Команда	*OBJOPR	*EXECUTE
	Файл DDM	*USE	*EXECUTE
SLTCMD ¹	Команда	Любые права доступа	*USE
WRKCMD ²	Команда	Любые права доступа	*USE
¹ Необходимо быть владельцем объекта или иметь какие-либо права доступа к объекту. ² Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией. ³ Необходимы права на выполнение (*X) к каталогам пути создаваемого файла и права на запись и выполнение (*WX) к родительскому каталогу создаваемого файла.			

Команды управления фиксацией

В этой таблице перечислены права доступа, необходимые для выполнения команд управления фиксацией.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
COMMIT			
ENDCMTCTL	Очередь сообщений, указанная в ключевом слове NFYOBJ соответствующей команды STRCMTCTL.	*OBJOPR, *ADD	*EXECUTE
ROLLBACK			
STRCMTCTL	Очередь сообщений, если указана в ключевом слове NFYOBJ	*OBJOPR, *ADD	*EXECUTE
	Область данных, указанная в ключевом слове NFYOBJ соответствующей команды STRCMTCTL	*CHANGE	*EXECUTE
	Файлы, указанные в ключевом слове NFYOBJ соответствующей команды STRCMTCTL	*OBJOPR *READ	*EXECUTE
WRKCMDFN ¹			
¹ Любой пользователь может применять эту команду для определений фиксации, принадлежащих заданию, выполняющемуся под управлением профайла этого пользователя. Пользователи со специальными правами на управление заданиями (*JOBCTL) могут применять эту команду для любых определений фиксации.			

Команды исходной информации связи

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы исходной информацией связи.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGCSI	Объект исходной информации связи	*USE, *OBJMGT	*EXECUTE
	Описание устройства ¹	*CHANGE	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTCSI	Объект исходной информации связи		*READ, *ADD
	Описание устройства ¹	*CHANGE	
DLTCSI	Объект исходной информации связи	*OBJEXIST	*EXECUTE
DSPCSI	Объект исходной информации связи	*READ	*EXECUTE
WRKCSI	Объекты исходной информации связи	*USE	*EXECUTE
¹ Права доступа проверяются при обращении к объекту исходной информации связи.			

Команды настройки

В этой таблице перечислены права доступа, необходимые для выполнения команд настройки.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
PRTDEVADR	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства	*USE	*EXECUTE
RSTCFG (Q) ⁵	Все объекты, заменяемые при восстановлении	*OBJEXIST ¹	*EXECUTE
	Целевая библиотека		*ADD, *EXECUTE ¹
	Пользовательский профайл, которому принадлежат создаваемые объекты	*ADD ¹	
	Лентопротяжное устройство	*USE	*EXECUTE
	Файл магнитной ленты (QSYSTAP)	*USE ¹	*EXECUTE
	Файл сохранения (если указан)	*USE	*EXECUTE
	Вывод на принтер (QPSRLDSP), если указано output(*print)	*USE	*EXECUTE
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Файл описания полей AQSYS/QASRRSTO, если указан несуществующий файл вывода	*USE	*EXECUTE
RTVCFGSTS	Объект	*OBJOPR	*EXECUTE
RTVCFGSRC	Объект	*USE	*EXECUTE
	Исходный файл	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SAVCFG ²	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE
	Файл сохранения (если в нем есть записи)	*USE, *ADD, *OBJMGT	*EXECUTE
SAVRSTCFG	В исходной системе - те же права доступа, которые необходимы для команды SAVCFG.		
	В целевой системе - те же права доступа, которые необходимы для команды RSTCFG.		
VRYCFG ^{3, 5, 6, 7}	Объект	*USE, *OBJMGT	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
WRKCFGSTS ⁴	Объект	*OBJOPR	*EXECUTE
¹	Если пользователю предоставлены специальные права доступа *SAVSYS, то указанные права доступа не нужны.		
²	Необходимы специальные права доступа *SAVSYS.		
³	Если пользователю предоставлены специальные права доступа *JOBCTL, то права доступа к объекту не нужны.		
⁴	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
⁵	Для того чтобы присвоить параметру Разрешить различия в объектах (ALWOBJDIF) значение, отличное от *NONE, или указать RESETSYS(*YES), необходимы специальные права доступа *ALLOBJ.		
⁶	Если объект - это библиотека носителей и указано состояние *ALLOCATE или *DEALLOCATE, то необходимы специальные права доступа *IOSYSCFG.		
⁷	Для применения этой команды с параметром GENPTHCERT(*YES) необходимы специальные права доступа *IOSYSCFG и *SECADM.		

Команды списка конфигураций

В этой таблице перечислены права доступа, необходимые для выполнения команд списка конфигураций.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDCFGLE ²	Список конфигурации	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGGL ²	Список конфигурации	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGLE ²	Список конфигурации	*CHANGE, *OBJMGT	*EXECUTE
CPYCFGGL ²	Список конфигурации	*USE, *OBJMGT	*ADD
CRTCFGGL ²	Список конфигурации		
DLTCFGL	Список конфигурации	*OBJEXIST	*EXECUTE
DSPCFGL ²	Список конфигурации	*USE, *OBJMGT	*EXECUTE
RMVCFGLE ²	Список конфигурации	*CHANGE, *OBJMGT	*EXECUTE
WRKCFGL ^{1,2}	Список конфигурации	*OBJOPR	*EXECUTE
¹	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
²	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.		

Команды списка соединений

В этой таблице перечислены права доступа, необходимые для выполнения команд списка соединений.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTCNNL	Список соединений	*OBJEXIST	*EXECUTE
DSPCNNL	Список соединений	*USE	*EXECUTE
WRKCNNL ¹	Список соединений	*OBJOPR	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.			

Команды для работы с описанием контроллера

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием контроллера.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGCTLAPPC ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Описание линии (SWTLINLST)	*USE	*EXECUTE
	Список соединений (CNLSTOUT)	*USE	*EXECUTE
CHGCTLASC ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Описание линии (SWTLINLST)	*USE	*EXECUTE
CHGCTLBSC ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Описание линии (SWTLINLST)	*USE	*EXECUTE
CHGCTLFNC ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Описание линии (SWTLINLST)	*USE	*EXECUTE
CHGCTLHOST ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Описание линии (SWTLINLST)	*USE	*EXECUTE
	Список соединений (CNLSTOUT)	*USE	*EXECUTE
CHGCTLLWS ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Программа (INZPGM)	*USE	*EXECUTE
CHGCTLNET ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLRTL ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Описание линии (SWTLINLST)	*USE	*EXECUTE
CHGCTLRWS ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
	Описание линии (SWTLINLST)	*USE	*EXECUTE
	Список соединений (CNLSTOUT)	*USE	*EXECUTE
CHGCTLTAP ²	Описание контроллера	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLVWS ²	Контроллер	*CHANGE, *OBJMGT	*EXECUTE
CRTCTLAPPC ²	Описание линии (LINE или SWTLINLST)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Список соединений (CNLSTOUT)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLASC ²	Описание линии (LINE или SWTLINLST)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTCTLBSC ²	Описание линии (LINE или SWTLINLST)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLFNC ²	Описание линии (LINE или SWTLINLST)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLHOST ²	Описание линии (LINE или SWTLINLST)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Список соединений (CNLSTOUT)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLLWS ²	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		
	Программа (INZPGM)	*USE	*EXECUTE
CRTCTLNET ²	Описание линии (LINE)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLRTL ²	Описание линии (LINE или SWTLINLST)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLRWS ²	Описание линии (LINE или SWTLINLST)	*USE	*EXECUTE
	Описание устройства (DEV)	*USE	*EXECUTE
	Список соединений (CNLSTOUT)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLTAP ²	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		
CRTCTLVWS ²	Описание устройства (DEV)	*USE	*EXECUTE
	Описание контроллера		
DLTCTLD	Описание контроллера	*OBJEXIST	*EXECUTE
DSPCTLD	Описание контроллера	*USE	*EXECUTE
ENDCTLRCY	Описание контроллера	*USE	*EXECUTE
PRTCMNSEC ³			
RSMCTLRCY	Описание контроллера	*USE	*EXECUTE
WRKCTLD ¹	Описание контроллера	*OBJOPR	*EXECUTE
¹	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
²	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.		
³	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ и *IOSYSCFG, либо права доступа *AUDIT.		

Команды шифрования

В этой таблице перечислены права доступа, необходимые для выполнения команд шифрования.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDCKMKSFE	Пользовательский пользователь	*ADD, *OBJOPR, *READ	
	Пользовательская библиотека		*EXECUTE
	Пользовательский каталог	*X	
	Пользовательский потоковый файл	*R	
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	Очередь сообщений QHST	*OBJOPR, *ADD	*EXECUTE
ADDMSTPART (Q) ¹			
CHGCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Очередь сообщений QHST	*OBJOPR, *ADD	*EXECUTE
CHGMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Очередь сообщений QHST	*OBJOPR, *ADD	*EXECUTE
CHKMSTKVV (Q) ¹			
CLRMSTKEY (Q) ¹			
CPHDTA (Q)			
CRTCKMKSF	Пользовательская библиотека		*ADD, *EXECUTE
DSPCKMKSFE	Пользовательский пользователь	*OBJOPR, *READ	
	Пользовательская библиотека		*EXECUTE
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCKMKSFE	Пользовательский пользователь	*ADD, *OBJOPR, *READ	
	Пользовательская библиотека		*EXECUTE
GENCPHK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	QCRP/QPCRGEX *FILE	*OBJOPR, *READ	*EXECUTE
	Очередь сообщений QHST	*OBJOPR, *ADD	*EXECUTE
GENMAC (Q)			
GENPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
RMVCKMKSFE	Пользовательский пользователь	*DLT, *OBJOPR	
	Пользовательская библиотека		*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RMVCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *DLT	*EXECUTE
	Очередь сообщений QHST	*OBJOPR, *ADD	*EXECUTE
SETMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Очередь сообщений QHST	*OBJOPR, *ADD	*EXECUTE
SETMSTKEY (Q) ¹			
TRNCKMKSF	Пользовательский пользователь	*OBJOPR, *READ, *UPD	
	Пользовательская библиотека		*EXECUTE
TRNPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
VFYMSTK (Q)	Очередь сообщений QHST	*OBJOPR, *ADD	*EXECUTE
VFYPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, READ	*EXECUTE
¹ Для выполнения этой команды необходимы специальные права доступа *ALLOBJ и *SECADM.			

Команды для работы с областью данных

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с областью данных.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGDTAARA ¹	Области данных	*CHANGE	*EXECUTE
CRTDTAARA ¹	Области данных		*READ, *ADD
	Описание устройства APPC ⁴	*CHANGE	
DLTDTAARA	Области данных	*OBJEXIST	*EXECUTE
DSPDTAARA	Области данных	*USE	*EXECUTE
RTVDTAARA ²	Области данных	*USE	*EXECUTE
WRKDTAARA ³	Области данных	Любые права доступа	*USE
¹ Эти права доступа необходимы, даже если команды изменения и создания области данных запускаются с помощью функций языка высокого уровня, хотя права доступа к самой команде в этом случае не требуются. ² Права доступа проверяются при запуске, а не при компиляции. ³ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции. ⁴ Права доступа проверяются при обращении к области данных.			

Команды для работы с очередью данных

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с очередью данных.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTDTAQ	Очередь данных		*READ, *ADD
	Целевая очередь данных для программы QSNDDTAQ	*OBJOPR, *ADD	*EXECUTE
	Исходная очередь данных для программы QRCVDTAQ	*OBJOPR, *READ	*EXECUTE
	Описание устройства APPC ²	*CHANGE	
DLTDTAQ	Очередь данных	*OBJEXIST	*EXECUTE
WRKDTAQ ¹	Очередь данных	*READ	*USE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией. ² Права доступа проверяются при обращении к области данных.			

Команды для работы с описанием устройств

В этой таблице перечислены права доступа, необходимые для выполнения команд с для работы с описанием устройств.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CFGDEVMLB ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGASPA (Q)			
CHGASPACT (Q) ⁷	Описание устройства	*USE	
CHGDEVAPPC ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
	Описание режима (MODE)	*USE	*EXECUTE
CHGDEVASC ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVASP ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVBSC ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVCRP ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDKT ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDSP ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
	Принтер (PRINTER)	*USE	*EXECUTE
CHGDEVFNC ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVHOST ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVINTR ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNET ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNWSH ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVOPT ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVPR ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
	Контрольный список (если указан)	*READ	*EXECUTE
CHGDEVRTL ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNPT ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGDEVSNUF ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVTAP ⁴	Описание устройства	*CHANGE, *OBJMGT	*EXECUTE
CRTDEVAPPC ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
	Описание режима (MODE)	*USE	*EXECUTE
CRTDEVASC ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVASP ⁴	Описание устройства		*EXECUTE
CRTDEVBSC ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVCRP ⁴	Описание устройства		*EXECUTE
CRTDEVDKT ⁴	Описание устройства		*EXECUTE
CRTDEVDSP ⁴	Описание принтера (PRINTER)	*USE	*EXECUTE
	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVFNC ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVHOST ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVINTR ⁴	Описание устройства		
CRTDEVMLB ⁴	Описание устройства		*EXECUTE
CRTDEVNET ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVNWSH ⁴	Описание устройства		*EXECUTE
CRTDEVOPT ⁴	Описание устройства		*EXECUTE
CRTDEVPR ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
	Контрольный список (если указан)	*READ	*EXECUTE
CRTDEVRTL ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVSNPT ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVSNUF ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
CRTDEVTAP ⁴	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание устройства		
DLTDEVD ¹	Описание устройства	*OBJEXIST	*EXECUTE
DSPASPSTS	Описание устройства	*USE	
DSPCNNSTS	Описание устройства	*OBJOPR	*EXECUTE
DSPDEV	Описание устройства	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ENDASPBAL (Q)			
ENDDEVRCY	Описание устройства	*USE	*EXECUTE
HLDCMNDEV ²	Описание устройства	*OBJOPR	*EXECUTE
PRTCMNSEC ^{4, 5}			
RLSCMNDEV	Описание устройства	*OBJOPR	*EXECUTE
RSMDEVRCY	Описание устройства	*USE	*EXECUTE
SETASPGRP ⁶	Все описания устройств в группе ASP	*USE	
	Будут изменены все указанные библиотеки в списке библиотек перед пространством имен библиотек и список библиотек	*USE	
STRASPBAL (Q)			
TRCASPBAL (Q)			
WRKDEVD ³	Описание устройства	*OBJOPR	*EXECUTE
1	Для удаления связанной очереди вывода требуются права к существованию объекта (*OBJEXIST) по отношению к очереди вывода и права на выполнение (*EXECUTE) библиотеки QUSRSYS.		
2	Необходимы специальные права на управление заданиями (*JOBCTL) и операционные права доступа к описанию устройства.		
3	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
4	Для запуска этой команды требуются специальные права доступа *IOSYSCFG.		
5	Для запуска этой команды требуются специальные права доступа *ALLOBJ.		
6	Если значение *CURUSR задано в параметре Группа ASP (ASPGRP) или Библиотеки для текущей нити (USRLIBL), то вам также необходимы права на чтение (*READ) к описанию задания, указанному в вашем пользовательском профайле, и права на выполнение (*EXECUTE) к библиотеке этого описания задания.		
7	Для выполнения этой команды необходимы специальные права доступа *JOBCTL.		

Команды для работы с эмуляцией устройств

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с эмуляцией устройств.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDEMLCFGE	Файл конфигурации эмуляции	*CHANGE	*EXECUTE
CHGEMLCFGE	Файл конфигурации эмуляции	*CHANGE	*EXECUTE
EJTEMLOUT	Описание устройства эмуляции, если указано	*OBJOPR	*EXECUTE
	Описание устройства эмуляции, если указано расположение	*OBJOPR	*EXECUTE
ENDPRTEML	Описание устройства эмуляции, если указано	*OBJOPR	*EXECUTE
	Описание устройства эмуляции, если указано расположение	*OBJOPR	*EXECUTE
EMLPRTKEY	Описание устройства эмуляции, если указано	*OBJOPR	*EXECUTE
	Описание устройства эмуляции, если указано расположение	*OBJOPR	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
EML3270	Описание устройства эмуляции	*OBJOPR	*EXECUTE
	Описание контроллера эмуляции	*OBJOPR	*EXECUTE
RMVEMLCFGE	Файл конфигурации эмуляции	*CHANGE	*EXECUTE
STREML3270	Файл конфигурации эмуляции	*OBJOPR	*EXECUTE
	Устройство эмуляции, описание контроллера эмуляции, устройство рабочей станции и описание контроллера рабочей станции.	*OBJOPR	*EXECUTE
	Описание принтера, пользовательская программа выхода и таблицы перевода (если указано)	*OBJOPR	*EXECUTE
STRPRTEML	Файл конфигурации эмуляции	*OBJOPR	*EXECUTE
	Описания устройства эмуляции и контроллера эмуляции	*OBJOPR	*EXECUTE
	Описание принтера, вывод на принтер, очередь сообщений, описание задания, очередь заданий и таблицы перевода (если указано)	*OBJOPR	*EXECUTE
SNDEMLIGC	Исходный файл	*OBJOPR	*EXECUTE
TRMPRTEML	Описание устройства эмуляции	*OBJOPR	*EXECUTE

Команды для работы с каталогами и теневыми каталогами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с каталогами и теневыми каталогами.

Для выполнения следующих команд не требуются никакие права доступа к объектам:			
ADDDIRE ² ADDDIRSHD ¹ CHGSYSDIRA ² CHGDIRE ³	CHGDIRSHD ¹ CPYFRMDIR ¹ CPYTODIR ¹ DSPDIRE	ENDDIRSHD ⁴ RMVDIRE ¹ RMVDIRSHD ¹ RNMDIRE ²	STRDIRSHD ⁴ WRKDIRE ^{3,5} WRKDIRLOC ^{1,5} WRKDIRSHD ^{1,5}
¹	Необходимы специальные права доступа *SECADM.		
²	Необходимы специальные права доступа *SECADM или *ALLOBJ.		
³	Пользователь со специальными правами доступа *SECADM может работать со всеми записями каталога. Все остальные пользователи могут работать только со своими записями.		
⁴	Необходимы специальные права доступа *JOBCTL.		
⁵	Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.		

Команды для работы с сервером каталогов

В этой таблице перечислены права доступа, необходимые для выполнения команд с сервером каталогов.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGDIRSRVA ¹			
CPYTOLDIF ²	Потоковый файл LDIF (если он уже существует)	*STMF	*W, *OBJEXIST, *OBJMGT
	Родительский каталог потокового файла LDIF	*DIR	*WX
CPYFRMLDIF ²	Потоковый файл LDIF	*STMF	*R
	Родительский каталог потокового файла LDIF	*DIR	*X
DB2LDIF ²	Потоковый файл LDIF (если он уже существует)	*STMF	*W, *OBJEXIST, *OBJMGT
	Родительский каталог потокового файла LDIF	*DIR	*WX
LDIF2DB ²	Потоковый файл LDIF	*STMF	*R
	Родительский каталог потокового файла LDIF	*DIR	*X
¹ Необходимы специальные права доступа *ALLOBJ и *IOSYSCFG. ² Для выполнения этой команды необходимо выполнение одного из следующих условий: <ul style="list-style-type: none"> • Наличие специальных прав доступа *ALLOBJ и *IOSYSCFG. • Указание DN администратора и пароля • Наличие прав администратора сервера каталогов 			

Команды для работы с дисками

В этой таблице перечислены права доступа, необходимые для команд работы с дисками.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам:			
ENDDSKRGZ (Q) ¹	STRDSKRGZ (Q) ¹	WRKDSKSTS	
¹ Для выполнения этой команды необходимы специальные права доступа *ALLOBJ.			

Команды для удаленного входа в систему дисплейной станции

В этой таблице перечислены права доступа, необходимые для выполнения команд для удаленного входа в систему дисплейной станции.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ENDPASTHR			
STRPASTHR	Устройство APPC в исходной системе	*CHANGE	*EXECUTE
	Устройство APPC в целевой системе	*CHANGE	*EXECUTE
	Виртуальный контроллер в целевой системе ¹	*USE	*EXECUTE
	Виртуальное устройство в целевой системе ^{1,2}	*CHANGE	*EXECUTE
	Программа, указанная в системном значении QRMTSIGN целевой системы (если указана) ¹	*USE	*USE
TFRPASTHR			
<p>¹ Эти права доступа должны быть предоставлены пользовательскому профайлу, запустившему пакетное задание удаленного входа в систему. Если при удаленном входе в систему пропускается меню входа в систему, то применяется пользовательский профайл, указанный в параметре удаленного пользователя (RMTUSER). Если выполняется обычная процедура входа в систему (RMTUSER(* NONE)), то выбирается пользовательский профайл по умолчанию, который указан в записи средств связи подсистемы, обрабатывающей запрос на удаленный вход в систему. Обычно это пользовательский профайл QUSER.</p> <p>² Если выполняется обычная процедура входа в систему, то профайлу, выбранному в меню входа в систему в целевой системе, должны быть предоставлены права доступа к этому объекту.</p>			

Команды рассылки

В этой таблице перечислены права доступа, необходимые для выполнения команд рассылки.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			
CHGDSTD ¹	Документ ²	*CHANGE	*EXECUTE
CHGDSTQ (Q)			
CHGDSTRTE (Q)			
DLTDST ¹			
DSPDSTLOG (Q)	Журналы	*USE	*EXECUTE
	Получатели журналов	*USE	*EXECUTE
DSPDSTSRV (Q)			
HLDDSTQ (Q)			
INZDSTQ (Q)			
QRYDST ¹	Запрошенный файл	*CHANGE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RCVDST ¹	Запрошенный файл	*CHANGE	*EXECUTE
	Папки	*CHANGE	*EXECUTE
RLSDSTQ (Q)			
RMVDSTQ (Q)			
RMVDSTRTE (Q)			
RMVDSTSYSN (Q)			
SNDDST ¹	Запрошенный файл или документ	*USE	*EXECUTE
SNDDSTQ (Q)			
WRKDSTQ (Q)			
WRKDPCQ (Q)			
¹ Если пользователь запрашивает рассылку для другого пользователя, то ему должны быть предоставлены права на работу от имени этого пользователя. ² Если рассылка зарегистрирована.			

Команды для работы с списком рассылки

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с списком рассылки.

Для выполнения следующих команд не требуются никакие права доступа к объектам:			
ADDDSTLE ¹ CHGDSTL ¹	CRTDSTL DLTDSTL ¹	DSPDSTL RMVDSTLE ¹	RNMDSTL ¹ WRKDSTL ²
¹ Необходимо иметь специальные права доступа *SECADM или быть владельцем списка рассылки. ² Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.			

Команды для работы с объектом библиотеки документов

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с объектом библиотеки документов.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDDLOAUT	Объект библиотеки документов	*ALL или принадлежность	*EXECUTE
CHGDLOAUD ¹			
CHGDLOAUT	Объект библиотеки документов	*ALL или принадлежность	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGDLOOWN	Объект библиотеки документов	Принадлежность или *ALLOBJ	*EXECUTE
	Прежний пользовательский профайл	*DLT	*EXECUTE
	Новый пользовательский профайл	*ADD	*EXECUTE
CHGDLOPGP	Объект библиотеки документов	Принадлежность или *ALLOBJ	*EXECUTE
	Профайл старой основной группы	*DLT	*EXECUTE
	Профайл новой основной группы	*ADD	*EXECUTE
CHGDOCD ²	Описание документа	*CHANGE	*EXECUTE
CHKDLO ²	Объект библиотеки документов	В соответствии с ключевым словом AUT	*EXECUTE
CHKDOC	Документы	*CHANGE	*EXECUTE
	Орфографический словарь	*CHANGE	*EXECUTE
CPYDOC	Исходный документ	*USE	*EXECUTE
	Целевой документ, если заменяется существующий документ	*CHANGE	*EXECUTE
	Целевая папка, если создается новый целевой документ	*CHANGE	*EXECUTE
CRTDOC	Содержащая объект папка	*CHANGE	*EXECUTE
CRTFLR	Содержащая объект папка	*CHANGE	*EXECUTE
DLTDLO ³	Объект библиотеки документов	*ALL	*EXECUTE
DLTDOCL ²⁰	Список документов	*ALL ⁴	*EXECUTE
DMPDLO ¹⁵			
DSPAUTLDLO	Список прав доступа	*USE	*EXECUTE
	Объект библиотеки документов	*USE	*EXECUTE
DSPDLOAUD ²¹	Файл вывода, если он указан	См. общие правила.	См. общие правила.
DSPDLOAUT	Объект библиотеки документов	*USE или принадлежность	*EXECUTE
DSPDLONAM ²²	Объект библиотеки документов	*USE	*EXECUTE
DSPDOC	Документы	*USE	*EXECUTE
DSPFLR	Папки	*USE	*EXECUTE
EDTDLOAUT	Объект библиотеки документов	*ALL или принадлежность	*EXECUTE
EDTDOC	Документы	*CHANGE	*EXECUTE
FILDOC ²	Запрошенный файл	*USE	*EXECUTE
	Папки	*CHANGE	*EXECUTE
MOVDOC	Исходная папка (если исходный документ расположен в папке)	*CHANGE	*EXECUTE
	Исходный документ	*ALL	*EXECUTE
	Целевая папка	*CHANGE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
MRGDOC ⁵	Документы	*USE	*EXECUTE
	Исходная папка	*USE	*EXECUTE
	Целевой документ, если заменяется существующий документ	См. общие правила.	См. общие правила.
	Целевая папка, если создается новый целевой документ	См. общие правила.	См. общие правила.
PAGDOC	Документы	*CHANGE	*EXECUTE
PRTDOC	Папки	*USE	*EXECUTE
	Документы	*USE	*EXECUTE
	Команды DLTPF, DLTF и DLTOVR, если указана инструкция <i>INDEX</i>	*USE	*EXECUTE
	Команды CRTPF, OVRPRTF, DLTSPLF и DLTOVR, если указана инструкция <i>RUN</i>	*USE	*EXECUTE
	Документ с сохраненными данными, если указано SAVOUTPUT (*YES)	*USE	*EXECUTE
	Папка сохранения, если указано SAVOUTPUT(*YES)	*USE	*EXECUTE
QRYDOCLIB ^{2,6}	Запрошенный файл	*USE	*EXECUTE
	Список документов (если существует)	*CHANGE	*EXECUTE
RCLDLO	Объект библиотеки документов		
	Внутренние документы, либо все документы и папки ¹⁶		
RGZDLO	Объект библиотеки документов	*CHANGE или принадлежность	*EXECUTE
	DLO(*ALL), DLO(*ALL) FLR(*ANY) или DLO(*ALL) FLR(*ANY) MAIL(*YES) ¹⁶		
RMVDLOAUT	Объект библиотеки документов	*ALL или принадлежность	*EXECUTE
RNMDLO	Объект библиотеки документов	*ALL	*EXECUTE
	Содержащая объект папка	*CHANGE	*EXECUTE
RPLDOC ²	Запрошенный файл	*READ	*EXECUTE
	Документы	*CHANGE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RSTDLO (Q) ^{7, 8, 9}	Объект библиотеки документов (при замене существующего объекта)	*ALL ¹⁰	*EXECUTE
	Родительская папка, если создается новый DLO	*CHANGE ¹⁰	*EXECUTE
	Профайл владельца, если создается новый DLO	*ADD ¹⁰	*EXECUTE
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Файл сохранения	*USE	*EXECUTE
	Файл оптического носителя (OPTFILE) ¹⁷	*R	Не применимо
	Путь к файлу оптического носителя (OPTFILE) ¹⁷	*X	Не применимо
	Оптический том ¹⁹	*USE	Не применимо
	Лентопротяжное устройство и оптический накопитель	*USE	*EXECUTE
RSTS36FLR ^{11,12,14}	Папка S/36	*USE	*EXECUTE
	Целевая папка	*CHANGE	*EXECUTE
	Файл устройства или описание устройства	*USE	*EXECUTE
RTVDLONAM ²²	Объект библиотеки документов	*USE	*EXECUTE
RTVDOC ²	Документ (если изымается)	*CHANGE	*EXECUTE
	Документ (если не изымается)	*USE	*EXECUTE
	Запрошенный файл	*CHANGE	*EXECUTE
SAVDLO ^{7,13}	Объект библиотеки документов	*ALL ¹⁰	*EXECUTE
	Лентопротяжное устройство и оптический накопитель	*USE	*EXECUTE
	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE
	Файл сохранения (если в нем есть записи)	*USE, *ADD, *OBJMGT	*EXECUTE
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Файл оптического носителя (OPTFILE) ¹⁷	*RW	Не применимо
	Каталог файла оптического носителя (OPTFILE) ¹⁷	*WX	Не применимо
	Путь к файлу оптического носителя (OPTFILE) ¹⁷	*X	Не применимо
	Корневой каталог (/) тома ^{17, 18}	*RWX	Не применимо
	Оптический том ¹⁹	*CHANGE	Не применимо
SAVRSTDLO	В исходной системе - те же права доступа, которые необходимы для команды SAVDLO.		
	В целевой системе - те же права доступа, которые необходимы для команды RSTDLO.		
WRKDOC	Папки	*USE	
WRKFLR	Папки	*USE	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
1	Необходимы специальные права доступа *AUDIT.		
2	Если один пользователь работает от имени другого пользователя, то проверяются права доступа к объекту второго пользователя.		
3	Для удаления папки и всех находящихся в ней объектов необходимы права доступа *ALL ко всем объектам этой папки.		
4	При наличии специальных прав доступа *ALLOBJ или *SECADM все права доступа (*ALL) к списку библиотек документов не требуются.		
5	У вас должны быть права доступа к объекту, который играет роль исходного объекта при вставке. Например, если указано MRGTYPE(*QRY), то вам необходимы права на использование запроса, заданного в параметре QRYDFN.		
6	В списке документов или файле вывода будут показаны только те объекты, которые соответствуют критериям запроса и по отношению к которым у вас есть права доступа не ниже *USE.		
7	У вас должны быть специальные права доступа *SAVSYS, *ALLOBJ или вы должны быть зарегистрированы в системном каталоге рассылки.		
8	Для использования сочетания параметров RSTDLO DLO(*MAIL) необходимы специальные права доступа *SAVSYS или *ALLOBJ.		
9	Для того чтобы присвоить параметру Разрешить различия в объектах (ALWOBJDIF) значение, отличное от *NONE, необходимы специальные права доступа *ALLOBJ.		
10	Если пользователю предоставлены специальные права доступа *SAVSYS или *ALLOBJ, то указанные права доступа не нужны.		
11	Для замены документа необходимы все (*ALL) права доступа к этому документу. Для восстановления новой информации в папке необходимы операционные права доступа к папке и все права доступа к данным папки, либо специальные права доступа *ALLOBJ.		
12	Если применяется к словарю данных, то достаточно прав на выполнение команды.		
13	Следующие сочетания параметров разрешено указывать только при наличии специальных прав доступа *SAVSYS или *ALLOBJ: <ul style="list-style-type: none"> • SAVDLO DLO(*ALL) FLR(*ANY) • SAVDLO DLO(*MAIL) • SAVDLO DLO(*CHG) • SAVDLO DLO(*SEARCH) OWNER(не *CURRENT) 		
14	Если исходная папка является папкой документов, то пользователь должен быть зарегистрирован в системном каталоге рассылки.		
15	Для создания дампа внутренних объектов библиотеки документов необходимы специальные права доступа *ALLOBJ.		
16	Необходимы специальные права доступа *ALLOBJ или *SECADM.		
17	Права доступа проверяются только для оптических носителей в формате UDF.		
18	Эти права доступа проверяются только при очистке оптического тома.		
19	Оптические тома фактически не являются объектами системы. Связь между оптическим томом и списком прав доступа, применяемым для ограничения доступа к тому, устанавливается функцией поддержки оптической памяти.		
20	У вас должны быть специальные права доступа *ALLOBJ в случае OWNER(*ALL) или OWNER(имя), если это имя другого пользователя.		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
21	Для выполнения этой команды необходимы специальные права доступа ко всем объектам (*ALLOBJ) или специальные права на контроль (*AUDIT).		
22	Для выполнения этой команды со значением *DST в качестве искомого класса объектов необходимы специальные права доступа ко всем объектам (*ALLOBJ).		

Команды для работы с DNS

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с доменными именами (DNS).

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHKDNSCFG ¹	Существующий файл конфигурации	*R	
	Путь к существующему файлу конфигурации	*X	
	Существующий файл вывода	*W	
	Путь к существующему файлу вывода	*X	
	Родительский объект нового файла вывода	*RX	
CHKDNSZNE ¹	Существующий файл зоны	*R	
	Путь к существующему файлу зоны	*X	
	Существующий файл вывода	*W	
	Путь к существующему файлу вывода	*X	
	Родительский объект нового файла вывода	*RX	
CRTRNDCCFG ¹	Существующий исходный файл энтропии	*R	
	Путь к существующему исходному файлу энтропии	*X	
	Существующий файл вывода	*W	
	Путь к существующему файлу вывода	*X	
	Родительский объект нового файла вывода	*RX	
RUNDNSUPD	Существующий пакетный файл ввода	*R	
	Путь к существующему пакетному файлу ввода	*X	
	Существующий файл ключей	*R	
	Путь к существующему файлу ключей	*X	
	Существующий файл вывода	*W	
	Путь к существующему файлу вывода	*X	
	Родительский объект нового файла вывода	*RX	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RUNRNDCCMD	Существующий файл конфигурации RNDC	*R	
	Путь к существующему файлу конфигурации RNDC	*X	
	Существующий файл ключей	*R	
	Путь к существующему файлу ключей	*X	
	Существующий файл вывода	*W	
	Путь к существующему файлу вывода	*X	
	Родительский объект нового файла вывода	*RX	
STRDIGQRY	Существующий пакетный файл ввода	*R	
	Путь к существующему пакетному файлу ввода	*X	
	Существующий файл доверенных ключей	*R	
	Путь к существующему файлу доверенных ключей	*X	
	Существующий файл ключей	*R	
	Путь к существующему файлу ключей	*X	
	Существующий файл вывода	*W	
	Путь к существующему файлу вывода	*X	
	Родительский объект нового файла вывода	*RX	
STRHOSTQRY	Существующий файл вывода	*W	
	Путь к существующему файлу вывода	*X	
	Родительский объект нового файла вывода	*RX	

¹ Для запуска этой команды требуются специальные права доступа *IOSYSCFG.

Команды для двухбайтовых кодировок

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с двухбайтовыми кодировками.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CPYIGCTBL	Таблица сортировки DBCS (*IN)	*ALL	*EXECUTE
	Таблица сортировки DBCS (*OUT)	*USE	*EXECUTE
CRTIGCDCT	Словарь преобразования DBCS		*READ, *ADD
DLTIGCDCT	Словарь преобразования DBCS	*OBJEXIST	*EXECUTE
DLTIGCSRT	Таблица сортировки DBCS	*OBJEXIST	*EXECUTE
DLTIGCTBL	Таблица шрифтов DBCS	*OBJEXIST	*EXECUTE
DSPIGCDCT	Словарь преобразования DBCS	*USE	*EXECUTE
EDTIGCDCT	Словарь преобразования DBCS	*USE, *UPD	*EXECUTE
	Пользовательский словарь	*ADD, *DLT	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRCGU	Таблица сортировки DBCS	*CHANGE	*EXECUTE
	Таблица шрифтов DBCS	*CHANGE	*EXECUTE
STRFMA	Таблица шрифтов DBCS (если указана опция копирования в таблицу)	*OBJOPR, *READ *ADD, *UPD	*EXECUTE
	Таблица шрифтов DBCS (если указана опция копирования из таблицы)	*OBJOPR, *READ	*EXECUTE
	Рабочий файл средства управления шрифтами (QGPL/QAFSVDf)	*CHANGE	*EXECUTE

Команды описания формата

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием формата.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTEDTD	Описание формата		*EXECUTE, *ADD
DLTEDTD	Описание формата	*OBJEXIST	*EXECUTE
DSPEDTD	Описание формата	*OBJOPR	*EXECUTE
WRKEDTD ¹	Описание формата	Любые права доступа	*USE

¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.

Команды для работы с переменными среды

В этой таблице перечислены права доступа, необходимые для выполнения команд с переменными среды.

Для выполнения следующих команд не требуются никакие права доступа к объектам.			
ADDENVVAR ¹	CHGENVVAR ¹	RMVENVVAR ¹	WRKENVVAR ¹

¹ Для обновления переменных среды уровня системы необходимы специальные права доступа *JOBCTL.

Команды настройки расширенной беспроводной локальной сети

В этой таблице перечислены права доступа, необходимые для выполнения команд настройки расширенной беспроводной локальной сети.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDEWCBCDE	Исходный файл	*USE	*EXECUTE
ADDEWCM	Исходный файл	*USE	*EXECUTE
ADDEWCPTCE	Исходный файл	*USE	*EXECUTE
ADDEWLM	Исходный файл	*USE	*EXECUTE
CHGEWCBCDE	Исходный файл	*USE	*EXECUTE
CHGEWCM	Исходный файл	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGEWCPTCE	Исходный файл	*USE	*EXECUTE
CHGEWLM	Исходный файл	*USE	*EXECUTE
DSPEWCBCDE	Исходный файл	*USE	*EXECUTE
DSPEWCM	Исходный файл	*USE	*EXECUTE
DSPEWCPTCE	Исходный файл	*USE	*EXECUTE
DSPEWLM	Исходный файл	*USE	*EXECUTE
RMVEWCBCDE	Исходный файл	*USE	*EXECUTE
RMVEWCPTCE	Исходный файл	*USE	*EXECUTE

Команды для работы с файлами

В этой таблице перечислены права доступа, необходимые для выполнения команд с файлами.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDICFDEVE	файл ICF	*OBJOPR, *OBJMGT	*EXECUTE
ADDLFM	Логический файл	*OBJOPR, *OBJMGT или *OBJALTER	*EXECUTE, *ADD
	Файл, указанный в параметре DTAMBRS, если для логического файла определен ключ	*OBJOPR, *OBJMGT или *OBJALTER	*EXECUTE
	Файл, указанный в параметре DTAMBRS, если для логического файла не определен ключ	*OBJOPR	*EXECUTE
ADDPFCST	Зависимый файл, если указан параметр TYPE(*REFCST)	*OBJMGT или *OBJALTER	*EXECUTE
	Родительский файл, если указан параметр TYPE(*REFCST)	*OBJMGT или *OBJREF	*EXECUTE
	Файл, если указан параметр TYPE(*UNQCST) или TYPE(*PRIKEY)	*OBJMGT	*EXECUTE
ADDPFM	Физический файл	*OBJOPR, *OBJMGT или *OBJALTER	*EXECUTE, *ADD
ADDPFTRG	Физический файл (для вставки триггера)	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Физический файл (для удаления триггера)	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Физический файл (для обновления триггера)	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Программа триггера	*EXECUTE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGDDMF	Файл DDM	*OBJOPR, *OBJMGT	*EXECUTE
	Описание устройства ⁷	*CHANGE	
CHGDKTF	Файл дискеты	*OBJOPR, *OBJMGT	*EXECUTE
	Устройство, если в команде указано имя устройства	*OBJOPR	*EXECUTE
CHGDSPF	Файл дисплея	*OBJOPR, *OBJMGT	*EXECUTE
	Устройство, если указано имя устройства	*OBJOPR	*EXECUTE
CHGDTA	Файл данных	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Программа	*USE	*EXECUTE
	Файл дисплея	*USE	*EXECUTE
CHGICFDEVE	файл ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGICFF	файл ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGLF	Логический файл	*OBJMGT или *OBJALTER	*EXECUTE
CHGLFM	Логический файл	*OBJMGT или *OBJALTER	*EXECUTE
CHGPF	Физический файл	*OBJMGT или *OBJALTER	*EXECUTE
CHGPF CST	Зависимый файл	*OBJMGT или *OBJALTER	*EXECUTE
CHGPFM	Физический файл	*OBJMGT или *OBJALTER	*EXECUTE
CHGPFTRG	Физический файл	*OBJMGT или *OBJALTER	*EXECUTE
CHGPRTF	Вывод на принтер	*OBJOPR, *OBJMGT	*EXECUTE
	Устройство, если указано имя устройства	*OBJOPR	*EXECUTE
CHGSAVF	Файл сохранения	*OBJOPR и (*OBJMGT или *OBJALTER).	*EXECUTE
CHGSRCPF	Исходный физический файл	*OBJMGT или *OBJALTER	*EXECUTE
CHGTAPF	Файл магнитной ленты	*OBJOPR, *OBJMGT	*EXECUTE
	Устройство, если указано имя устройства	*OBJOPR	*EXECUTE
CLRPFM	Физический файл	*OBJOPR, *OBJMGT или *OBJALTER, *DLT	*EXECUTE
CLRSAVF	Файл сохранения	*OBJOPR, *OBJMGT	*EXECUTE
CPYF	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой файл (файл устройства)	*OBJOPR, *READ	*EXECUTE
	Целевой файл (физический файл)	См. общие правила.	См. общие правила.
	Базовый файл, если исходный файл - это логический файл	*READ	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
SPYFRMDKT	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой файл (файл устройства)	*OBJOPR, *READ	*EXECUTE
	Целевой файл (физический файл)	См. общие правила.	См. общие правила.
SPYFRMIMPF	Исходный файл	*OBJOPR, *READ	*USE
	Целевой файл (файл устройства)	*OBJOPR, *READ	*USE
	Целевой файл (физический файл)	См. общие правила.	См. общие правила.
	Базовый файл, если исходный файл - это логический файл	*READ	*USE
	Команда CRTDDMF	*USE	*USE
SPYFRMQRYF ¹	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой файл (файл устройства)	*OBJOPR, *READ	*EXECUTE
	Целевой файл (физический файл)	См. общие правила.	См. общие правила.
SPYFRMSTMF	Потоковый файл	*R	
	Каталоги, указанные в префиксе пути к потоковому файлу	*X	
	Целевой файл базы данных, если указан параметр MBROPT(*ADD)	*WX	*X
	Целевой файл базы данных, если указан параметр MBROPT(*REPLACE или *NONE)	*WX, *OBJMGT	*X
	Целевой файл базы данных (при создании нового элемента)	*WX	*X, *ADD
	Таблица преобразования *TBL, применяемая при преобразовании данных	*R	*X
	Существующий целевой файл сохранения	*RWX, *OBJMGT	*X
	Создаваемый целевой файл сохранения		*RWX
SPYFRMTAP	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой файл (файл устройства)	*OBJOPR, *READ	*EXECUTE
	Целевой файл (физический файл)	См. общие правила.	См. общие правила.
SPYSRCF	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой файл (файл устройства)	*OBJOPR, *READ	*EXECUTE
	Целевой файл (физический файл)	См. общие правила.	См. общие правила.
SPYTODKT	Исходный файл и целевой файл	*OBJOPR, *READ	*EXECUTE
	Устройство, если в команде указано имя устройства	*OBJOPR, *READ	*EXECUTE
	Базовый физический файл, если исходный файл - это логический файл	*READ	*EXECUTE
SPYTOIMPF	Исходный файл	*OBJOPR, *READ	*USE
	Целевой файл (файл устройства)	*OBJOPR, *READ	*USE
	Целевой файл (физический файл)	См. общие правила.	См. общие правила.
	Базовый файл, если исходный файл - это логический файл	*READ	*USE
	Команда CRTDDMF	*USE	*USE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
СРЮТОСТМФ	Файл базы данных или файл сохранения	*RX	*X
	Потоковый файл, если он уже существует	*W	
	Родительский каталог потокового файла, если потоковый файл не существует	*WX	
	Префикс пути к потоковому файлу	*X	
	Файл базы данных и потоковый файл, если указан AUT(*FILE) или AUT(*INDIRFILE)	*OBJMGT	
	Таблица преобразования *TBL, применяемая при преобразовании данных	*R	*X
СРЮТОТАР	Исходный файл и целевой файл	*OBJOPR, *READ	*EXECUTE
	Устройство, если указано имя устройства	*OBJOPR, *READ	*EXECUTE
	Базовый физический файл, если исходный файл - это логический файл	*READ	*EXECUTE
CRTDDMF	Файл DDM: REPLACE(*NO)		*READ, *ADD
	Файл DDM: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Описание устройства ⁷	*CHANGE	
CRTDKTF	Устройство, если указано имя устройства	*OBJOPR	*EXECUTE
	Файл дискеты: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Файл дискеты: REPLACE(*YES)	См. общие правила.	*READ, *ADD, *EXECUTE
CRTDSPF	Исходный файл	*USE	*EXECUTE
	Устройство, если указано имя устройства	*OBJOPR	*EXECUTE
	Файл, указанный в ключевых словах REF и REFFLD	*OBJOPR	*EXECUTE
	Файл дисплея: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Файл дисплея: REPLACE(*YES)	См. общие правила.	*READ, *ADD, *EXECUTE
CRTICFF	Исходный файл	*USE	*EXECUTE
	Файл, указанный в ключевых словах REF и REFFLD	*OBJOPR	*EXECUTE
	Файл ICF: REPLACE(*NO)		*READ, *ADD
	Файл ICF: REPLACE(*YES)	См. общие правила.	*READ, *ADD

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTLF	Исходный файл	*USE	*EXECUTE
	Файл, указанный в ключевом слове PFILE или JFILE, если для логического файла определен ключ	*OBJOPR, *OBJMGT или *OBJALTER	*EXECUTE
	Файл, указанный в ключевом слове PFILE или JFILE, если для логического файла не определен ключ	*OBJOPR	*EXECUTE
	Файлы, указанные в ключевых словах FORMAT и REFACCPH	*OBJOPR	*EXECUTE
	Таблицы, указанные в ключевом слове ALTSEQ	*OBJOPR	*EXECUTE
	Логический файл		*EXECUTE, *ADD
	Файл, указанный в параметре DTAMBRS, если для логического файла определен ключ	*OBJOPR, *OBJMGT или *OBJALTER	*EXECUTE
	Файл, указанный в параметре DTAMBRS, если для логического файла не определен ключ	*OBJOPR	*EXECUTE
CRTPF	Исходный файл	*USE	*EXECUTE
	Файлы, указанные в ключевых словах FORMAT и REFFLD, и таблицы, указанные в ключевом слове ALTSEQ	*OBJOPR	*EXECUTE
	Физический файл		*EXECUTE, *ADD
CRTPRTF	Исходный файл	*USE	*EXECUTE
	Устройство, если указано имя устройства	*OBJOPR	*EXECUTE
	Файлы, указанные в ключевых словах REF и REFFLD	*OBJOPR	*EXECUTE
	Вывод на принтер: Replace(*NO)		*READ, *ADD, *EXECUTE
	Вывод на принтер: Replace(*YES)	См. общие правила.	*READ, *ADD, *EXECUTE
CRTSAVF	Файл сохранения		*READ, *ADD, *EXECUTE
CRTSRCPF	Исходный физический файл		*READ, *ADD, *EXECUTE
CRTS36DSPF	Исходный файл приемника, если TOMBR не равно *NONE	*ALL	*CHANGE
	Исходный файл QS36SRC	*USE	*EXECUTE
	Файл дисплея: REPLACE(*NO)		*READ, *ADD
	Файл дисплея: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Команда Создать файл дисплея (CRTDSPF)	*OBJOPR	*EXECUTE
CRTTAPF	Файл магнитной ленты: REPLACE(*NO)		*READ, *ADD
	Файл магнитной ленты: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Устройство, если указано имя устройства	*OBJOPR	*EXECUTE
DLTF	Файл	*OBJOPR, *OBJEXIST	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DSPCPCST	Файл базы данных с ограничениями, ожидающими проверки	*OBJOPR, *READ	*EXECUTE
DSPDBR	Файл базы данных	*OBJOPR	*EXECUTE
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
DSPDDMF	Файл DDM	*OBJOPR	
DSPDTA	Файл данных	*USE	*EXECUTE
	Программа	*USE	*EXECUTE
	Файл дисплея	*USE	*EXECUTE
DSPFD ²	Файл	*OBJOPR	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
	Файл, если это физический файл и указан параметр TYPE(*ALL, *MBR или *MBRLST)	Права доступа к данным, отличные от *EXECUTE	*EXECUTE
DSPFFD	Файл	*OBJOPR	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
DSPPFM	Физический файл	*USE	*EXECUTE
DSPSAVF	Файл сохранения	*USE	*EXECUTE
EDTGPCST	Область данных, указанная в ключевом слове NFYOBJ соответствующей команды STRCMTCTL.	*CHANGE	*EXECUTE
	Файлы, указанные в ключевом слове NFYOBJ соответствующей команды STRCMTCTL.	*OBJOPR, *ADD	*EXECUTE
GENCAT	Файл базы данных	*OBJOPR и права доступа к данным, отличные от *EXECUTE	*EXECUTE
INZPFM	Физический файл, если указан параметр RECORD(*DFT)	*OBJOPR, *OBJMGT или *OBJALTER, *ADD	*EXECUTE
	Физический файл, если указан параметр RECORD(*DLT)	*OBJOPR, *OBJMGT или *OBJALTER, *ADD, *DLT	*EXECUTE
MRGSRC	Целевой файл	*CHANGE, *OBJMGT	*CHANGE
	Файл обслуживания	*USE	*EXECUTE
	Корневой файл	*USE	*EXECUTE
OPNDBF	Файл базы данных	*OBJOPR и права доступа к данным, отличные от *EXECUTE	*EXECUTE
OPNQRYF	Файл базы данных	*OBJOPR и права доступа к данным, отличные от *EXECUTE	*EXECUTE
PRTRGPGM ¹¹			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RGZPFM	Файл, содержащий элемент	*OBJOPR, *OBJMGT или *OBJALTER, *READ, *ADD, *UPD, *DLT, *EXECUTE	*EXECUTE
RMVICFDEVE	файл ICF	*OBJOPR, *OBJMGT	*EXECUTE
RMVM	Файл, содержащий элемент	*OBJEXIST, *OBJOPR	*EXECUTE
RMVPCST	Файл	*OBJMGT или *OBJALTER	*EXECUTE
RMVPFTRG	Физический файл	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	Файл, содержащий элемент	*OBJOPR, *OBJMGT	*EXECUTE, *UPD
RSTS36F ⁴ (Q)	Целевой файл	*ALL	См. общие правила.
	Исходный файл	*USE	*EXECUTE
	Базовый физический файл, если восстанавливаемый файл - это логический (альтернативный) файл	*CHANGE	*EXECUTE
	Описание устройства для дискеты или магнитной ленты	*USE	*EXECUTE
RTVMBRD	Файл	*USE	*EXECUTE
SAVSAVFDTA	Описание лентопротяжного устройства, дисковод или оптического накопителя	*USE	*EXECUTE
	Файл сохранения	*USE	*EXECUTE
	Оптический файл сохранения/восстановления ⁸ (если он уже существует)	*RW	Не применимо
	Родительский каталог файла OPTFILE ⁸	*WX	Не применимо
	Префикс пути к файлу OPTFILE ⁸	*X	Не применимо
	Корневой каталог (/) оптического тома ^{8,9}	*RWX	Не применимо
	Оптический том ¹⁰	*CHANGE	Не применимо
SAVS36F	Исходный файл	*USE	*EXECUTE
	Целевой файл, если это физический файл	*ALL	См. общие правила.
	Файл устройства или описание устройства	*USE	*EXECUTE
SAVS36LIBM	Целевой файл, если это физический файл	*ALL	См. общие правила.
	Исходный файл	*USE	*EXECUTE
	Файл устройства или описание устройства	*USE	*EXECUTE
STRAPF ³	Исходный файл	*OBJMGT, *CHANGE	*READ, *ADD
	Команды CRTPF, CRTLF, ADDPFM, ADDLFM и RMVM	*USE	*EXECUTE
STRDFU ³	Программа (если выбрана опция создания программы)		*READ, *ADD
	Программа (если выбрана опция изменения или удаления программы)	*OBJEXIST	*READ, *ADD
	Файл (при изменении или просмотре данных)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Файл (при просмотре данных)	*READ	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
UPDDTA	Файл	*CHANGE	*EXECUTE
WRKDDMF ³	Файл DDM	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD
WRKF ^{3,5}	Файл	*OBJOPR	*USE
WRKPCFCST ³			*EXECUTE
1	<p>В команде CPYFRMQRYP используется параметр FROMOPNID, а не FROMFILE. Пользователю должны быть предоставлены достаточные права доступа, чтобы перед запуском команды CPYFRMQRYP можно было выполнить команду OPNQRYP. Если в команде CPYFRMQRYP указан параметр CRTFILE(*YES), то при определении прав доступа к новому целевому файлу в качестве исходного файла будет рассматриваться первый файл, указанный в параметре FILE соответствующей команды OPNQRYP.</p>		
2	<p>Для выполнения этой команды вы должны быть владельцем файла или иметь операционные права доступа.</p>		
3	<p>Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.</p>		
4	<p>Если создается новый файл, и для этого файла существует владелец прав доступа, то у пользователя должны быть все права доступа (*ALL) к владельцу прав доступа, либо владелец прав доступа должен принадлежать этому пользователю. Если владелец прав доступа не существует, то владельцем файла станет пользователь, запустивший команду RSTS36F, а общие права доступа станут равны *ALL.</p>		
5	<p>Требуются какие-либо права доступа к объекту.</p>		
6	<p>Необходимы специальные права доступа *ALLOBJ.</p>		
7	<p>Права доступа проверяются при обращении к файлу DDM.</p>		
8	<p>Наличие этих прав доступа проверяется только для оптических носителей формата UDF.</p>		
9	<p>Эти права доступа проверяются только при очистке оптического тома.</p>		
10	<p>Оптические тома фактически не являются объектами системы. Связь между оптическим томом и списком прав доступа, применяемым для ограничения доступа к тому, устанавливается функцией поддержки оптической памяти.</p>		
11	<p>Для выполнения этой команды необходимы специальные права доступа *ALLOBJ или *AUDIT.</p>		

Команды для работы с фильтром

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с фильтром.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDALRACNE	Фильтрация	*USE, *ADD	*EXECUTE
ADDALRSLTE	Фильтрация	*USE, *ADD	*EXECUTE
ADDPBACNE	Фильтрация	*USE, *ADD	*EXECUTE
ADDPBLSLTE	Фильтрация	*USE, *ADD	*EXECUTE
CHGALRACNE	Фильтрация	*USE, *UPD	*EXECUTE
CHGALRSLTE	Фильтрация	*USE, *UPD	*EXECUTE
CHGFTR	Фильтрация	*OBJMGT	*EXECUTE
CHGPRBACNE	Фильтрация	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Фильтрация	*USE, *UPD	*EXECUTE
CRTFTR	Фильтрация		*READ, *ADD

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTFTR	Фильтрация	*OBJEXIST	*EXECUTE
RMVFTRACNE	Фильтрация	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Фильтрация	*USE, *DLT	*EXECUTE
WRKFTR ¹	Фильтрация	Любые права доступа	*EXECUTE
WRKFTRACNE ¹	Фильтрация	*USE	*EXECUTE
WRKFTRSLTE ¹	Фильтрация	*USE	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.			

Финансовые команды

В этой таблице перечислены права доступа, необходимые для выполнения финансовых команд.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
SBMFNCJOB (Q)	Описание задания и очередь сообщений ¹	*OBJOPR	*EXECUTE
SNDFNCIMG (Q)	Описание задания и очередь сообщений ¹	*OBJOPR	*EXECUTE
WRKDEVTBL (Q)	Описание устройства ¹	Не менее одного типа прав доступа к данным	*EXECUTE
WRKPGMTBL (Q)			
WRKUSRTBL (Q)			
¹ Эти права доступа должны быть предоставлены пользовательскому профайлу QFNC.			

Команды для графических операций i5/OS

В этой таблице перечислены права доступа, необходимые для выполнения команд для графических операций i5/OS.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGFCNUSG ⁵			
DSPFCNUSG			
EDTWSOAUT	Объект рабочей станции ¹	*OBJMGT ^{2,3,4}	*EXECUTE
GRTWSOAUT	Объект рабочей станции ¹	*OBJMGT ^{2,3,4}	*EXECUTE
RVKWSOAUT	Объект рабочей станции ¹	*OBJMGT ^{2,3,4}	*EXECUTE
SETCSTDTA	Исходный пользовательский профайл	*CHANGE	*EXECUTE
	Целевой пользовательский профайл	*CHANGE	*EXECUTE
WRKFCNUSG			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
1	Объект рабочей станции - это внутренний объект, который создается при установке компонента графических операций i5/OS. Он поставляется с общими правами доступа *USE.		
2	Вы должны быть владельцем объекта, либо у вас должны быть права доступа *OBJMGT, а также предоставляемые или аннулируемые права доступа.		
3	Для того чтобы вы могли предоставить права доступа *OBJMGT или *AUTLMGT, вы должны быть владельцем, либо у вас должны быть права доступа *ALLOBJ.		
4	Для защиты объекта рабочей станции с помощью списка прав доступа или для удаления списка прав доступа необходимы следующие права доступа: <ul style="list-style-type: none"> • Права владельца объекта рабочей станции. • Права доступа *ALL к объекту рабочей станции. • Специальные права доступа *ALLOBJ. 		
5	Для изменения прав доступа к функции необходимы специальные права доступа администратора защиты (*SECADM).		

Команды для работы с набором графических символов

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с набором графических символов.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTGSS	Исходный файл	*USE	*EXECUTE
	Набор графических символов		*READ, *ADD
DLTGSS	Набор графических символов	*OBJEXIST	*EXECUTE
WRKGSS ¹	Набор графических символов	*OBJOPR	*USE
1 Необходимо быть владельцем объекта или иметь какие-либо права доступа к объекту.			

Команды для сервера хоста

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с сервером хоста.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам.			
ENDHOSTSVR (Q)		STRHOSTSVR (Q)	

Команды для работы с каталогом образов

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с каталогом образов.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Тип объекта	Необходимые права доступа	
			К объекту	К библиотеке ¹
ADDIMGCLGE	Каталог образов	*IMGCLG	*CHANGE	*EXECUTE
	Префикс пути к каталогу образов	*DIR	*X	
	Имя устройства, если задан FROMDEV	*DEV	*USE	
	Файл образов, если задан FROMFILE	*STMF	*R, *OBJMGT	
	Префикс пути к файлу образов, если задан FROMFILE	*DIR	*X	
	Родительский каталог файла образов, если задан FROMFILE	*DIR	*RX	
CHGIMGCLG	Каталог образов	*IMGCLG	*CHANGE	*EXECUTE
	Префикс пути к каталогу образов	*DIR	См. общие правила	
	Префикс пути к новому каталогу образов, если задан DIR	*DIR	См. общие правила	
CHGIMGCLGE	Каталог образов	*IMGCLG	*CHANGE	*EXECUTE
	Префикс пути к каталогу образов	*DIR	См. общие правила	
CRTIMGCLG	QUSRSYS	*LIB		*READ, *ADD
	Каталог образов, если задано DIR(*REFIMGCLG)	*IMGCLG	*USE	*OBJOPR, *READ, *ADD, *EXECUTE
	Префикс пути к каталогу образов ²	*DIR	См. общие правила	
DLTIMGCLG	Каталог образов	*IMGCLG	*OBJEXIST	*EXECUTE
	Префикс пути к каталогу образов	*DIR	См. общие правила	
LODIMGCLG	Каталог образов	*IMGCLG	*USE	*EXECUTE
	Каталог образов, если задано WRTPTC(*ALL) или WRTPTC(*NONE)	*IMGCLG	*CHANGE	*EXECUTE
	Виртуальное устройство	*DEV	*USE	
	Префикс пути к каталогу образов	*DIR	См. общие правила	
LODIMGCLGE	Каталог образов	*IMGCLG	*USE	*EXECUTE
	Префикс пути к каталогу образов	*DIR	См. общие правила	
RMVIMGCLGE	Каталог образов	*IMGCLG	*CHANGE	*EXECUTE
	Префикс пути к каталогу образов	*DIR	См. общие правила	
RTVIMGCLG	Каталог образов	*IMGCLG	*USE	*EXECUTE
	Описание устройства, если задан параметр DEV	*DEV	*USE	
VFYIMGCLG	Каталог образов	*IMGCLG	*USE	*EXECUTE
	Виртуальное устройство	*DEV	*USE	
	Префикс пути к каталогу образов	*DIR	См. общие правила	
WRKIMGCLG	Каталог образов	*IMGCLG	*USE	*EXECUTE
WRKIMGCLGE	Каталог образов	*IMGCLG	*USE	*EXECUTE

Команда	Объект	Тип объекта	Необходимые права доступа	
			К объекту	К библиотеке ¹
¹	Объекты каталога образов находятся в библиотеке QUSRSYS.			
²	Если создается каталог, то вам также необходимы права на запись (*W) к каталогу, в котором создается новый каталог.			

Команды интегрированной файловой системы

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с интегрированной файловой системой.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
ADDLNK	Объект когда указано LNKTYPE(*HARD)	*STMF	QOpenSys, корневая (/), UDFS	*OBJEXIST
	Родительский объект для новой связи	*DIR	QOpenSys, корневая (/), UDFS	*WX
	Префикс пути	См. общие правила.		

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
CHGATR	Объект, если задается атрибут, отличный от *USECOUNT, *ALWCKPWRT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV, *SCAN, *CRTOBJSCAN, *SETUID, *SETGID, *RSTRDRNMUNL, *CRTOBJAUD	Любой	Любая, за исключением QSYS.LIB	*W
	Объект, если задается атрибут *USECOUNT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV	Любой	Любая, за исключением QSYS.LIB	*OBJMGT
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	*X, *OBJMGT (права доступа, унаследованные от родительского объекта *FILE)
		другой	QSYS.LIB	*OBJMGT
	Объект, если задается атрибут *ALWCKPWRT	Любой	Все	*OBJMGT
	Каталог, содержащий объекты, если задан параметр SUBTREE(*ALL)	Любой каталог	Все	*RX
	Объект, если задаются следующие атрибуты: *CRTOBJSCAN или *SCAN ²⁶	*DIR и *STMF	QOpenSys, корневая (/), UDFS	
	Объект, если задаются следующие атрибуты: *SETUID, *SETGID, *RSTRDRNMUNL	Любой	Любая, за исключением QSYS.LIB и QDLS	Права владельца ¹⁵
*CRTOBJAUD ⁹				
Префикс пути ⁹	См. общие правила.			
CHGAUD ⁴				
CHGAUT	Объект	Все	QOpenSys, корневая (/), UDFS	Права владельца ¹⁵
			QSYS.LIB, QOPT ¹¹	Права владельца или *ALLOBJ
			QDLS	Права владельца, *ALL или *ALLOBJ
				*OBJMGT
	Оптический том	*DDIR	QOPT ⁸	*CHANGE
Каталог, содержащий объекты, если задан параметр SUBTREE(*ALL)	Любой каталог или библиотека	Все	*RX	
CHGCURDIR	Объект	Любой каталог		*R
	Оптический том	*DDIR	QOPT ⁸	*X
	Префикс пути	См. общие правила.		

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
CHGOWN ²⁴	Объект	Все	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Все	QOpenSys, корневая (/), UDFS	Права владельца и *OBJEXIST ¹⁵
		Все	QDLS	Права владельца или *ALLOBJ
			QOPT ¹¹	Права владельца или *ALLOBJ
CHGOWN ²⁴	Пользовательский профайл прежнего владельца - все, кроме QOPT, QDLS	*USRPRF	Все	*DLT
	Пользовательский профайл нового владельца - все, кроме QOPT	*USRPRF	Все	*ADD
	Оптический том	*DDIR	QOPT ⁸	*CHANGE
	Каталог, содержащий объекты, если задан параметр SUBTREE(*ALL)	Любой каталог или библиотека	Все	*RX
CHGPGP	Объект	Все	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Все	QOpenSys, корневая (/), UDFS	Права владельца ^{5, 15}
		Все	QDLS	Права владельца или *ALLOBJ
			QOPT ¹¹	Права владельца или *ALLOBJ
CHGPGP	Профайл прежней основной группы - все, кроме QOPT	*USRPRF	Все	*DLT
	Профайл новой основной группы - все, кроме QOPT	*USRPRF	Все	*ADD
	Оптический том	*DDIR	QOPT ⁸	*CHANGE
	Каталог, содержащий объекты, если задан параметр SUBTREE(*ALL)	Любой каталог или библиотека	Все	*RX

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
CHKIN	Объект, если тот, кто изъяс его - пользователь.	*STMF	QOpenSys, корневая (/), UDFS	*W
		*DOC	QDLS	*W
	Объект, если тот, кто изъяс его - не пользователь.	*STMF	QOpenSys, корневая (/), UDFS	*ALL, *ALLOBJ или права владельца
		*DOC	QDLS	*ALL, *ALLOBJ или права владельца
	Путь, если тот, кто изъяс объект - не пользователь.	*DIR	QOpenSys, корневая (/), UDFS	*X
	Каталог, содержащий объекты, если задан параметр SUBTREE(*ALL)	Любой каталог	Все	*RX
	Префикс пути	См. общие правила.		
CHKOUT	Объект	*STMF	QOpenSys, корневая (/), UDFS	*W
		*DOC	QDLS	*W
	Каталог, содержащий объекты, если задан параметр SUBTREE(*ALL)	Любой каталог	Все	*RX
	Префикс пути	См. общие правила.		

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
CPY ²⁵	Копируемый объект, исходный объект	Любой	QOpenSys, корневая (/), UDFS	*R и *OBJMGT или права владельца
		*DOC	QDLS	*RWX и *ALL или права владельца
		*MBR	QSYS.LIB	Нет
		другие	QSYS.LIB	*RX, *OBJMGT
		*DSTMF	QOPT ¹¹	*R
	Целевой объект, если указан параметр REPLACE(*YES) (если целевой объект уже существует)	Любой	Все ¹⁰	*W, *OBJEXIST, *OBJMGT
		*DSTMF	QOPT ¹¹	*W
		*LIB	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*FILE (PF или LF)	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*RWX, *ALL
	Копируемый каталог, который содержит объекты, если задан параметр SUBTREE(*ALL) (т.е. копируется содержимое каталога)	*DIR	QOpenSys, корневая (/), UDFS	*RX, *OBJMGT
CPY ²⁵	Путь к целевому объекту, родительский каталог целевого объекта	*FILE	QSYS.LIB	*RX, *OBJMGT
		*LIB	QSYS.LIB	*RX, *ADD
		*DIR	QOpenSys, корневая (/), UDFS	*WX
		*FLR	QDLS	*RWX
		*DDIR	QOPT ¹¹	*WX
	Исходный оптический том	*DDIR	QOPT ⁸	*USE
	Целевой оптический том	*DDIR	QOPT ⁸	*CHANGE

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
CPY ²⁵	Родительский каталог исходного объекта	*DIR	QOpenSys, корневая (/), UDFS	*X
		*FLR	QDLS	*X
		Другие	QSYS.LIB	*RX
		*DDIR	QOPT ¹¹	*X
	Префикс пути к целевому объекту	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, корневая (/), UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
	Префикс пути к исходному объекту	*DDIR	QOPT ¹¹	*X
	CPYFRMSTMF	См. раздел “Команды для работы с файлами” на стр. 404		
CPYTOSTMF	См. раздел “Команды для работы с файлами” на стр. 404			
CRTDIR ^{21, 22}	Родительский каталог	*DIR	QOpenSys, корневая (/), UDFS	*WX
		*FLR	QDLS	*CHANGE
		*FILE	QSYS.LIB	*RX, *ADD
		Любой		*ADD
		*DDIR	QOPT ¹¹	*WX
CRTDIR	Префикс пути	См. общие правила.		
	Оптический том	*DDIR	QOPT ⁸	*CHANGE
CVTDIR (Q) ¹⁶				
DSPAUT	Объект	Все	QDLS	*ALL
		Все	Все остальные	*OBJMGT или права владельца
		Все	QOPT ¹¹	Нет
	Оптический том	*DDIR	QOPT ⁸	*USE
	Префикс пути	См. общие правила.		
DSPCURDIR	Префикс пути	*DIR	QOpenSys, корневая (/), UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT ¹¹	*RX

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
DSPCURDIR	Текущий каталог	*DIR	QOpenSys, корневая (/), UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT ¹¹	*X
	Оптический том	*DDIR*	QOPT ⁸	*USE
DSPF	Файл базы данных	*FILE	QSYS.LIB	*USE
	Библиотека файла базы данных	*LIB	QSYS.LIB	*EXECUTE
	Потоковый файл	*STMF	QOpenSys, корневая (/), UDFS	*R
		*USRSPC	QSYS.LIB	*USE
		Префикс пути	См. общие правила.	
DSPLNK	Любой	Любой	Корневая (/), QOpenSys, UDFS QSYS.LIB ²⁷ , QDLS, QOPT ¹¹	Нет
	Файл, опция 12 (Работа со ссылками)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	корневая (/), QOpenSys, UDFS	*R
DSPLNK	Объект символической связи	*SYMLNK	корневая (/), QOpenSys, UDFS	Нет
	Оптический том	*DDIR	QOPT ⁸	*USE
	Родительский каталог упомянутого объекта - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
DSPLNK	Родительский каталог упомянутого объекта - Указан шаблон ¹³	*DIR	корневая (/), QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB ²⁷	*R
		*FLR	QDLS	*R
		*DDIR	QOPT ¹¹	*R
		*DDIR		*R
	Родительский каталог упомянутого объекта - опция 8 (Показать атрибуты)	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Родительский каталог упомянутого объекта - опция 12 (Работа со ссылками)	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*SYMLNK	корневая (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Префикс родительского каталога упомянутого объекта - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Префикс родительского каталога упомянутого объекта - Указан шаблон ¹³	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
DSPLNK	Префикс родительского каталога упомянутого объекта - Опция 8 (Показать атрибуты)	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Префикс родительского каталога упомянутого объекта - опция 12 (Работа со ссылками)	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*SYMLNK	корневая (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Относительный путь ¹⁴ : Текущий рабочий каталог, содержащий объект - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
	Относительный путь ¹⁴ : Текущий рабочий каталог, содержащий объект - Указан шаблон ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
DSPLNK	Относительный путь ¹⁴ : Префикс текущего рабочего каталога, содержащего объект - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
DSPLNK	Относительный путь ¹⁴ : Префикс текущего рабочего каталога, содержащего объект - Указан шаблон ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
DSPMFSINF	Объект	Любой	Любой	Нет
	Префикс пути	См. общие правила.		
EDTF	Файл базы данных, существующий элемент	*FILE	QSYS.LIB	*CHANGE
	Библиотека файла базы данных	*LIB	QSYS.LIB	*EXECUTE
	Файл базы данных, новый элемент	*FILE	QSYS.LIB	*CHANGE, *OBJMGT
	Библиотека файла базы данных, новый элемент	*LIB	QSYS.LIB	*EXECUTE, *ADD
	Потоковый файл, существующий файл	*STMF	QOpenSys, корневая (/), UDFS	*R
	Пользовательское пространство	*USRSPC	QSYS.LIB	*CHANGE
	Родительский каталог при создании потокового файла	*DIR	QOpenSys, корневая (/), UDFS	*WX
	Префикс пути	См. общие правила.		
ENDJRN	Объект	*DIR, если указано Subtree (*ALL)	QOpenSys, корневая (/), UDFS	*R, *X, *OBJMGT
		*DIR, если указано Subtree (*NONE), *SYMLNK, *STMF	QOpenSys, корневая (/), UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Родительский каталог	*DIR	QOpenSys, корневая (/), UDFS	*X
		*LIB	QSYS.LIB	*X
	Журналы	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Префикс пути	См. общие правила.		

1

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
MOV ¹⁹	Объект, перемещаемый в пределах одной файловой системы	*DIR	QOpenSys, корневая (/)	*OBJMGT, *W
		не *DIR	QOpenSys, корневая (/)	*OBJMGT
		*DOC	QDLS	*ALL
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	Нет
		другой	QSYS.LIB	Нет
		*STMF	QOPT ¹¹	*W
MOV	Путь к исходному объекту, родительский каталог	*DIR	QOpenSys, корневая (/), UDFS	*WX
		*FLR	QDLS	*RWX
		*FILE	QSYS.LIB, корневая (/)	*RX, *OBJEXIST
		другие	QOpenSys, корневая (/)	*RWX
	Путь к целевому объекту, родительский каталог	*DIR	QSYS.LIB	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *ADD, *DLT, *OBJMGT
		*LIB	QSYS.LIB	*RWX
		*DDIR	QOPT ¹¹	*WX
MOV	Префикс пути к целевому объекту	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	другие	*X
		*DDIR	QOPT ¹¹	*X
	Объект, перемещаемый из файловой системы в файловую систему QOpenSys, корневую (/) файловую систему или QDLS (поточный файл *STMF и *DOC, только *MBR).	*STMF	QOpenSys, корневая (/), UDFS	*R, *OBJEXIST, *OBJMGT
		*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	Не применимо
		*DSTMF	QOPT ¹¹	*RW
MOV	Перемещаемый в QSYS *MBR	*STMF	QOpenSys, корневая (/), UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT ¹¹	*RW

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
MOV	Оптический том (исходный и целевой)	*DDIR	QOPT ⁸	*CHANGE
	Исходный путь, перемещаемый из одной файловой системы в другую, родительский каталог	*DIR	QOpenSys, корневая (/), UDFS	*WX
		*FLR	QDLS	*X
		*FILE	QSYS.LIB	права владельца, *RX, *OBJEXIST
		*DDIR	QOPT ¹¹	*WX
Префикс пути	См. общие правила.			
RCLLNK ¹⁶				
RLSIFSLCK ¹⁸	объект	*STMF	корневая (/), QOpenSys, UDFS	*R
	Префикс пути	См. общие правила.		
RMVDIR ^{19,20}	Каталог	*DIR	QOpenSys, корневая (/), UDFS	*OBJEXIST
		*LIB	QSYS.LIB	*RX, *OBJEXIST
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*FLR	QDLS	*ALL
		*DDIR	QOPT ¹¹	*W
RMVDIR	Родительский каталог	*DIR	QOpenSys, корневая (/), UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT ¹¹	*WX
	Каталог, содержащий объекты, если задан параметр SUBTREE(*ALL)	Любой каталог	Все	*RX
	Оптический том	*DDIR	QOPT ⁸	*CHANGE
Префикс пути	См. общие правила.			
RMVLNK ¹⁹	Объект	*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*JRNRCV	QSYS.LIB	*OBJEXIST, *R
		другой	QSYS.LIB	*OBJEXIST
		*DSTMF	QOPT ¹¹	*W
		Любой	QOpenSys, корневая (/), UDFS	*OBJEXIST

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
RMVLNK	Родительский каталог	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, корневая (/), UDFS	*WX
		*DDIR	QOPT ¹¹	*WX
	Оптический том	*DDIR	QOPT ⁸	*CHANGE
	Префикс пути	См. общие правила.		
RNM ¹⁹	Объект	*DIR	QOpenSys, корневая (/), UDFS	*OBJMGT, *W
		не *DIR	QOpenSys, корневая (/), UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	Не применимо
		*FILE	QSYS.LIB	*OBJMGT, *OBJOPR
		другие	QSYS.LIB	*OBJMGT
	*DSTMF	QOPT ¹¹	*W	
Оптический том (исходный и целевой)	*DDIR	QOPT ⁸	*CHANGE	
RNM	Родительский каталог	*DIR	QOpenSys, корневая (/), UDFS	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *OBJMGT
		*LIB	QSYS.LIB	*X, *UPD
		*DDIR	QOPT ¹¹	*WX
	Префикс пути	*LIB	QSYS.LIB	*X, *UPD
		Любой	QOpenSys, корневая (/), UDFS, QDLS	*X

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
RST (Q) ^{23, 28, 30}	Объект, если он существует ²	Любой	QOpenSys, корневая (/), UDFS	*W, *OBJEXIST
			QSYS.LIB	Переменные ¹⁰
			QDLS	*ALL
	Префикс пути	См. общие правила.		
	Родительский каталог, создаваемый во время восстановления, когда задано CRTPRNDIR(*YES) ²	*DIR	QOpenSys, корневая (/), UDFS	*WX
Владелец родительского каталога, заданный в параметре PRNDIROWN ^{2, 6}	*USRPRF	QSYS.LIB	*ADD	
RST (Q)	Родительский каталог восстанавливаемого объекта ²	*DIR	QOpenSys, корневая (/), UDFS	*WX
	Родительский каталог восстанавливаемого объекта, если объект не существует ²	*FLR	QDLS	*CHANGE
		*DIR		*OBJMGT, *OBJALTER, *READ, *ADD, *UPD
	Пользовательский профайл, которому принадлежит новый восстанавливаемый объект ²	*USRPRF	QSYS.LIB	*ADD
	Лентопротяжное устройство, оптический накопитель или файл сохранения	*DEVVD, *FILE	QSYS.LIB	*RX
	Определение носителя	*MEDDFN	QSYS.LIB	*USE
RST (Q)	Библиотека для описания устройства, определения носителя или файла сохранения	*LIB	QSYS.LIB	*EXECUTE
	Файл вывода, если он указан	*STMF	QOpenSys, корневая (/), UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Префикс пути файла вывода	*DIR	QOpenSys, корневая (/), UDFS	*X
		*LIB	QSYS.LIB	*RX
RST (Q)	Оптический том при восстановлении с оптического накопителя	*DDIR	QOPT ⁸	*USE
	Префикс пути к оптическому каталогу и родительский каталог при восстановлении с оптического накопителя	*DDIR	QOPT ¹¹	*X
	Оптический файл при восстановлении с оптического накопителя	*DSTMF	QOPT ¹¹	*R

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
RTVCURDIR	Префикс пути	*DIR	QOpenSys, корневая (/), UDFS, QDLS, QOPT ¹¹	*RX
		*DDIR	QOPT ¹¹	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		Любой		*R
RTVCURDIR	Текущий каталог	*DIR	QOpenSys, корневая (/), UDFS, QOPT ¹¹	*X
		*DDIR	QOPT ¹¹	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Любой		*R
SAV ²⁹	Объект ²	Любой	QOpenSys, корневая (/), UDFS	*R, *OBJEXIST
			QSYS.LIB	Переменные ¹⁰
			QDLS	*ALL
	Префикс пути	См. общие правила.		
	Лентопротяжное устройство, оптический накопитель	*DEVVD	QSYS.LIB	*RX
Определение носителя	*MEDDFN	QSYS.LIB	*USE	
SAV	Файл сохранения, если он пуст	*FILE	QSYS.LIB	*USE, *ADD
	Файл сохранения, если он не пуст	*FILE	QSYS.LIB	*OBJMGT, *USE, *ADD
	Очередь сообщений о сохранении активных объектов	*MSGQ	QSYS.LIB	*OBJOPR, *ADD
	Библиотеки описания устройства, определения носителя, файла сохранения и очереди сообщений о сохранении активных объектов	*LIB	QSYS.LIB	*EXECUTE
SAV	Файл вывода, если он указан	*STMF	QOpenSys, корневая (/), UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Префикс пути файла вывода	*DIR	QOpenSys, корневая (/), UDFS	*X
		*LIB	QSYS.LIB	*RX

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
SAV	Оптический том при сохранении на оптическом накопителе	*DDIR	QOPT ⁸	*CHANGE
	Префикс пути к оптическому каталогу при сохранении на оптическом накопителе	*DDIR	QOPT ¹¹	*X
	Оптический родительский каталог при сохранении на оптическом накопителе	*DDIR	QOPT ¹¹	*WX
	Оптический файл (если он уже существовал ранее)	*DSTMF	QOPT ¹¹	*RW
SAVRST	В исходной системе - те же права доступа, что и для команды SAV.			
	В целевой системе - те же права доступа, что и для команды RST.			
STATFS	Объект	Любой	Любой	Нет
	Префикс пути	См. общие правила.		
STRJRN	Объект	*DIR, если указано Subtree (*ALL)	QOpenSys, корневая (/), UDFS	*R, *X, *OBJMGT
		*DIR, если указано subtree (*NONE), *SYMLNK, *STMF	QOpenSys, корневая (/), UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Родительский каталог	*DIR	QOpenSys, корневая (/), UDFS	*X
		*LIB	QSYS.LIB	*X
	Журналы	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Префикс пути	См. общие правила.		
WRKAUT ^{6,7}	Объект	*DOC или *FLR	QDLS	*ALL
		Все	не QDLS	*OBJMGT или права владельца
		*DDIR и *DSTMF	QOPT ¹¹	*NONE
	Оптический том	*DDIR	QOPT ⁸	*USE
	Префикс пути	См. общие правила.		

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
WRKLNK	Любой	Любой	Корневая (/), QOpenSys, UDFS, QSYS.LIB ²⁷ , QDLS, QOPT ¹¹	Нет
	Файл, опция 12 (Работа со ссылками)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	корневая (/), QOpenSys, UDFS	*R
	Объект символьной связи	*SYMLNK	корневая (/), QOpenSys, UDFS	Нет
	Оптический том	*DDIR	QOPT ⁸	*USE
WRKLNK	Родительский каталог упомянутого объекта - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Родительский каталог упомянутого объекта - Шаблон указан	*DIR	корневая (/), QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB ²⁷	*R
		*FLR	QDLS	*R
		*DDIR	QOPT ¹¹	*R
		*DDIR		*R
WRKLNK	Родительский каталог упомянутого объекта - опция 8 (Показать атрибуты)	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Родительский каталог упомянутого объекта - опция 12 (Работа со ссылками)	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*SYMLNK	корневая (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
WRKLNK	Префикс родительского каталога упомянутого объекта - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Префикс родительского каталога упомянутого объекта - Указан шаблон ¹³	*DIR	корневая (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Префикс родительского каталога упомянутого объекта - Опция 8 (Показать атрибуты)	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Префикс родительского каталога упомянутого объекта - опция 12 (Работа со ссылками)	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*SYMLNK	корневая (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
WRKLNK	Относительный путь ¹⁴ : Текущий рабочий каталог, содержащий объект - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
	Относительный путь ¹⁴ : Текущий рабочий каталог, содержащий объект - Указан шаблон ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
WRKLNK	Относительный путь ¹⁴ : Префикс текущего рабочего каталога, содержащего объект - Шаблон не указан ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
	Относительный путь ¹⁴ Префикс текущего рабочего каталога, содержащего объект - Указан шаблон ¹³	*DIR	корневая (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R

¹ Принятые права доступа не используются в командах интегрированной файловой системы.

² Если у вас есть специальные права доступа *SAVSYS, то вам не нужны права доступа, указанные для QSYS.LIB, QDLS, QOpenSys и корневой (/) файловой системы.

³ Необходимые права доступа зависят от типа объекта. См. описание QLIRNMO API . Если объект - это элемент базы данных, то ознакомьтесь с правами доступа, указанными для команды Переименовать элемент (RNMM).

⁴ Для изменения значения контроля необходимы специальные права доступа *AUDIT.

⁵ Если у запустившего команду пользователя нет прав доступа *ALLOBJ, то этот пользователь должен быть членом новой основной группы.

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
6 7 8 9 10	Если профайл, указанный в параметре PRNDIROWN, принадлежит не тому пользователю, который выполняет восстановление, то необходимы специальные права доступа *SAVSYS или *ALLOBJ. Для выполнения этих команд кроме перечисленных прав доступа необходимы права на выполнение команды DSPCURDIR. Оптические тома фактически не являются объектами системы. Связь между оптическим томом и списком прав доступа, применяемым для ограничения доступа к тому, устанавливается функцией поддержки оптической памяти. Для изменения атрибута *CRTOBJAUD необходимы специальные права доступа *AUDIT; обычные права доступа к префиксу пути (*X и *R) не нужны.			Необходимые права доступа зависят от команды. Ознакомьтесь с правами доступа, необходимыми для выполнения соответствующих команд SAVOBJ или RSTOBJ.
11 12 13 14 15	Права доступа, запрашиваемые QOPT для носителей в формате UDF. Права доступа *ADD необходимы только в том случае, если перемещаемый объект - *MRB. Шаблон: в некоторых командах в последнем компоненте полного имени можно указать звездочку (*) или вопросительный знак (?) для выполнения поиска по шаблону. Относительный путь: если путь начинается не с косой черты, то элементом пути, предшествующим первому подкаталогу, считается текущий рабочий каталог процесса. Например, если указан путь 'a/b', а текущий рабочий каталог - '/home/john', то команда обратится к объекту '/home/john/a/b'. Если пользователю предоставлены специальные права доступа *ALLOBJ, то указанные права доступа не нужны.			
16 17 18 19 20	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ. В приведенной выше таблице под QSYS.LIB понимаются как файловые системы QSYS.LIB из независимых ASP, так и файловая система QSYS.LIB. Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG. Если для каталога установлен атрибут ограничения изменения имен и удаления (бит S_ISVTX), то удаление связей с объектами из этого каталога будет разрешено только в следующих случаях: <ul style="list-style-type: none"> • Если пользователю предоставлены права доступа *ALLOBJ. • Если пользователю принадлежит объект, связь с которым удаляется. • Если пользователь является владельцем каталога. 			Если указан параметр RMVLNK (*YES), то у пользователя также должны быть права доступа *OBJEXIST ко всем объектам в данном каталоге.

Команда	Объект	Тип объекта	Файловая система	Необходимые права доступа к объекту ¹
21	Если для параметра CRTOBJAUD указано значение, отличное от *SYSVAL, то для QSYS.LIB, QOpenSys, корневой (/) и пользовательской файловых систем необходимы специальные права доступа *AUDIT (права на контроль).			
22	Для того чтобы пользователь мог задать значение параметра CRTOBJSCAN, отличное от *PARENT, у него должны быть права доступа ко всем объектам (*ALLOBJ) и права администратора защиты (*SECADM).			
23	Для того чтобы присвоить параметру Разрешить различия в объектах (ALWOBJDIF) значение, отличное от *NONE, необходимы специальные права доступа *ALLOBJ. Также необходимы специальные права доступа *SAVSYS или *ALLOBJ для присвоения значения *UDFS параметру RBDMFS.			
24	В случае изменения владельца потокового файла (*STMF) с прикрепленной программой на Java, во время выполнения которой проверяются права доступа и пользователя, и владельца, пользователю необходимы специальные права доступа ко всем объектам (*ALLOBJ) и специальные права доступа системного администратора (*SECADM).			
25	В случае копирования потокового файла (*STMF) с прикрепленной программой на Java, во время выполнения которой проверяются права доступа и пользователя, и владельца, пользователю необходимы специальные права доступа ко всем объектам (*ALLOBJ) и специальные права доступа администратора защиты (*SECADM).			
26	Для указания атрибутов *CRTOBJSCAN и *SCAN необходимы специальные права доступа ко всем объектам (*ALLOBJ) и специальные права доступа администратора защиты (*SECADM).			
27	При просмотре содержимого каталога /QSYS.LIB те объекты пользовательского профайла (*USRPRF), к которым у вызывающего нет никаких прав доступа (даже *EXCLUDE), не возвращаются.			
28	Для указания в параметре PVTAUT значения *YES необходимы специальные права доступа *ALLOBJ.			
29	Для указания в параметре PVTAUT значения *YES необходимы специальные права доступа *ALLOBJ или *SAVSYS.			
30	Необходимы специальные права доступа *SAVSYS или *ALLOBJ для присвоения значения *UDFS параметру RBDMFS.			

Команды интерактивного определения данных

В этой таблице перечислены права доступа, необходимые для выполнения команд интерактивного определения данных.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDDTADFN	Словарь данных	*CHANGE	*EXECUTE
	Файл	*OBJOPR, *OBJMGT	*EXECUTE
CRTDTADCT	Словарь данных		*READ, *ADD
DLTDTADCT ³	Словарь данных	OBJEXIST, *USE	
DSPDTADCT	Словарь данных	*USE	*EXECUTE
LNKDTADFN ¹	Словарь данных	*USE	*EXECUTE
	Файл	*OBJOPR, *OBJMGT	*EXECUTE
STRIDD			
WRKDTADCT ²	Словарь данных	*OBJOPR	*EXECUTE
WRKDBFIDD ²	Словарь данных	*USE ⁴	*EXECUTE
	Файл базы данных	*OBJOPR	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
WRKDTADFN ¹	Словарь данных	*USE, *CHANGE	*EXECUTE
¹	Для отключения файла не нужны права доступа к словарю данных.		
²	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
³	Перед тем как удалять словарь, необходимо отключить все подключенные файлы. Права доступа, необходимые для отключения файла, перечислены в описании команды LNKDTADFN.		
⁴	Для создания файла необходимы права на использование словаря данных. Для ввода данных в существующий файл права доступа к словарю данных не требуются.		

Команды для работы с Internetwork Packet Exchange (IPX)

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с Internetwork Packet Exchange (IPX).

Список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам, приведен в разделе Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTIPXD	Описание IPX	*OBJEXIST	*EXECUTE
DSPIPXD	Описание IPX	*USE	*EXECUTE
WRKIPXD	Описание IPX	*OBJOPR	*EXECUTE

Команды для работы с индексом поиска

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с индексом поиска.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDSCHIDX	Индекс поиска	*CHANGE	*USE
	Группа панелей	*USE	*EXECUTE
CHGSCHIDX	Индекс поиска	*CHANGE	*USE
CRTSCHIDX	Индекс поиска		*READ, *ADD
DLTSCHIDX	Индекс поиска	*OBJEXIST	*EXECUTE
RMVSCHIDX	Индекс поиска	*CHANGE	*USE
STRSCHIDX	Индекс поиска	*USE	*EXECUTE
WRKSCHIDX ¹	Индекс поиска	*ANY	*USE
WRKSCHIDX	Индекс поиска	*USE	*USE

Команды для работы с атрибутами IPL

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с атрибутами IPL.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам:	
CHGIPLA (Q) ¹	
DSP IPLA	
¹	Для выполнения этой команды необходимы специальные права доступа *SECADM и *ALLOBJ.

Команды Java

В этой таблице перечислены права доступа, необходимые для команд Java.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ANZJVM	Команда QSYS/STRSRVJOB	*USE	
	Команда QSYS/STRDBG	*USE	
DSPJVMJOB ¹	Задания виртуальной машины Java		
GENJVMDMP ¹			
PRTJVMJOB ¹			
WRKJVMJOB ¹			
¹	Для выполнения этой команды необходимы специальные права доступа *JOBCTL.		

Команды для работы с заданиями

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с заданиями.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
VSNJOB	Описание задания ^{9,11}	*USE	*EXECUTE
	Библиотеки в списке библиотек (системные, текущая и пользовательские) ⁷	*USE	
	Пользовательский профайл из описания задания ¹⁰	*USE	
	Таблица последовательности сортировки ⁷	*USE	*EXECUTE
	Очередь сообщений ¹⁰	*USE, *ADD	*EXECUTE
	Очередь заданий ^{10,11}	*USE	*EXECUTE
	Очередь вывода ⁷	*READ	*EXECUTE
CHGACGCDE ¹			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGGRPA ⁴	Очередь сообщений, если очередь сообщений связывается с группой	*OBJOPR	*EXECUTE
CHGJOB ^{1,2,3}	Новая очередь заданий (при изменении очереди заданий) ^{10,11}	*USE	*EXECUTE
	Новая очередь вывода (при изменении очереди вывода) ⁷	*READ	*EXECUTE
	Текущая очередь вывода (при изменении очереди вывода)	*READ	*EXECUTE
	Таблица последовательности сортировки ⁷	*USE	*EXECUTE
CHGPRJ	Пользовательский профайл для запроса на запуск программы, который применяется, если указано *PGMSTRRQS	*USE	*EXECUTE
	Пользовательский профайл и описание задания	*USE	*EXECUTE
CHGSYSJOB(Q) ¹³			
CHGUSRTRC ¹⁴	Буфер пользовательской трассировки, если указан параметр CLEAR(*YES). ¹⁵	*OBJOPR	*EXECUTE
	Буфер пользовательской трассировки, если задан параметр MAXSTG ¹⁵	*CHANGE, *OBJMGT	*USE
	Буфер пользовательской трассировки, если задан параметр TRCFULL. ¹⁵	*OBJOPR	*EXECUTE
DLTUSRTRC	Буфер пользовательской трассировки ¹⁵	*OBJOPR, *OBJEXIST	*EXECUTE
DLYJOB ⁴			
DMPUSRTRC	Буфер пользовательской трассировки ¹⁵	*OBJOPR	*EXECUTE
DSCJOB ¹			
DSPACTPJ	Описание устройства ASP	*USE	
	Библиотека программы		*EXECUTE
DSPJOB ¹			
DSPJOBTBL			
DSPJOBLOG ^{1,5}	Файл вывода и элемент существуют	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Элемент не существует	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *ADD
	Файл вывода не существует	*OBJOPR	*EXECUTE, *ADD
ENDGRPJOB			
ENDJOB ¹			
ENDJOBABN ¹			
ENDLOGSVR ⁶			
ENDPJ ⁶	Описание устройства ASP	*USE	
	Библиотека программы		*EXECUTE
HLDJOB ¹			
RLSJOB ¹			
RRTJOB			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RTVJOBA			
SBMDBJOB	Файл базы данных	*USE	*EXECUTE
	Очереди заданий	*READ	*EXECUTE
SBMDKTJOB	Очередь сообщений	*USE, *ADD	*EXECUTE
	Очередь заданий и описание устройства	*READ	*EXECUTE
SBMJOB ^{2, 12, 17, 18}	Описание задания ^{9,11}	*USE	*EXECUTE
	Библиотеки в списке библиотек (системные, текущая и пользовательские) ⁷	*USE	
	Очередь сообщений ¹⁰	*USE, *ADD	*EXECUTE
	Пользовательский профайл ^{10,11}	*USE	
	Пользовательский профайл из описания задания ¹⁰	*USE (на уровне 40)	
	Очередь заданий ^{10,11}	*USE	*EXECUTE
	Очередь вывода ⁷	*READ	*EXECUTE
	Таблица последовательности сортировки ⁷	*USE	*EXECUTE
	ASP в начальной группе ASP	*USE	
SBMNETJOB	Файл базы данных	*USE	*EXECUTE
STRLOGSVR ⁶			
STRPJ ⁶	Описание подсистемы	*USE	
	Программа	*USE	*EXECUTE
	Описание устройства ASP	*USE	
TFRBCHJOB	Очереди заданий	*READ	*EXECUTE
TFRGRPJOB	Первая групповая программа	*USE	*EXECUTE
TFRJOB ⁸	Очереди заданий	*USE	*EXECUTE
	Описание подсистемы, для которой выделена очередь заданий	*USE	
TFRSECJOB			
WRKACTJOB			
WRKARMJOB ¹⁶			
WRKASPJOB	Описание устройства	*USE	
WRKJOB ¹			
WRKJOBLOG			
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
1	Эти команды могут выполняться любым пользователем для заданий, запущенных с его собственным профайлом. Пользователь со специальными правами на управление заданиями (*JOBCTL) может выполнять эти команды для любого задания. При наличии специальных прав доступа *SPLCTL права доступа к очереди заданий не нужны. Однако необходимы права доступа к библиотеке, содержащей эту очередь.		
2	В вашем пользовательском профайле должны быть заданы права доступа, позволяющие работать с указанным приоритетом планирования и приоритетом вывода.		
3	Для изменения некоторых атрибутов даже в собственном задании необходимы специальные права на управление заданиями (*JOBCTL). Это следующие атрибуты: RUNPTY, TIMESLICE, PURGE, DFTWAIT и TSEPOOL.		
4	Эта команда влияет только на то задание, в котором она была задана.		
5	Для просмотра протокола задания, которому предоставлены права доступа ко всем объектам (*ALLOBJ), необходимы специальные права доступа *ALLOBJ или права на применение функции Протокол задания со всеми объектами операционной системы i5/OS, предоставленные через программу Администрирование приложений Навигатора System i. Изменить список пользователей, которым разрешено просматривать протокол задания со специальными правами доступа *ALLOBJ, можно и с помощью команды CHGFCNUSG (Изменить права доступа к функции), указав ИД функции QIBM_ACCESS_ALLOBJ_JOBLOG.		
6	Для выполнения этой команды необходимы специальные права на управление заданиями (*JOBCTL).		
7	У профайла, с которым выполняется задание, должны быть права доступа к указанному объекту. Принятые права доступа пользователя, передавшего задание на выполнение или изменившего его, не используются.		
8	При переходе к интерактивному заданию действуют следующие ограничения: <ul style="list-style-type: none"> • Очередь заданий, в которой находится задание, должна быть связана с активной подсистемой. • В описании новой подсистемы должна существовать запись о рабочей станции, связанной с заданием. • С рабочей станцией, связанной с заданием, не должно быть связано никаких других заданий, которые были приостановлены с помощью клавиши Sys Req (Системный запрос). Перед применением команды Перейти к заданию необходимо отменить приостановленные задания. • Задание не должно быть групповым. 		
9	Необходимые права доступа к указанному объекту должны быть и у пользователя, передавшего задание на выполнение, и у профайла, с которым будет выполняться задание.		
10	У пользователя, передавшего задание на выполнение, должны быть права доступа к указанному объекту.		
11	Используются принятые права доступа пользователя, запустившего команду CHGJOB или SBMJOB.		
12	У вас должны быть права доступа к пользовательскому профайлу и к описанию задания. У пользовательского профайла также должны быть права доступа к описанию задания.		
13	Для изменения некоторых атрибутов задания (даже в собственном задании пользователя) необходимы специальные права на управление заданиями (*JOBCTL) и специальные права доступа ко всем объектам (*ALLOBJ).		
14	Эти команды могут выполняться любым пользователем для заданий, запущенных с его собственным профайлом. Пользователь со специальными правами на управление заданиями (*JOBCTL) может выполнять эти команды для любого задания.		
15	Буфер пользовательской трассировки - это объект пользовательского пространства (*USRSPC) в библиотеке QUSRSYS с именем QPOZnnnnnn, где 'nnnnn' - номер задания, использующего пользовательскую функцию трассировки.		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
16	Для работы с заданием или просмотра сведений о задании необходимо выполнение одного из следующих условий: <ul style="list-style-type: none"> • Команда должна быть вызвана из задания. • Команда должна быть выполнена от лица пользовательского профайла, совпадающего с именем связанного с этим заданием пользователя. • Команда должна быть выполнена от лица пользовательского профайла, имеющего специальные права доступа к заданию (*JOBCTL). 		
17	Для указания строки кода учета ресурсов для параметра Код учета ресурсов (ACGCDE) необходимы права доступа (*USE) для команды Изменить код учета ресурсов (CHGACGCDE).		
18	Для использования параметра SBMFOR необходимо иметь специальные права доступа (*JOBCTL).		

Команды описания заданий

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием заданий.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGJOB	Описание задания	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Пользовательский профайл (USER)	*USE	
CPYAUDJRNE ⁸	Файл вывода уже существует	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE
	Файл вывода не существует		*EXECUTE *ADD
CRTJOB (Q)	Описание задания		*READ, *ADD
	Пользовательский профайл (USER)	*USE	
DLTJOB	Описание задания	*OBJEXIST	*EXECUTE
DSPJOB	Описание задания	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT ¹			
WRKJOB	Описание задания	Любой	*USE
¹ Для выполнения этой команды необходимы специальные права доступа *ALLOBJ или *AUDIT.			

Команды очереди заданий

В этой таблице перечислены права доступа, необходимые для команд очереди заданий.

Команда	Объект	Параметры очереди заданий ⁴		Специальные права доступа	Необходимые права доступа	
		AUTCHK	OPRCTL		К объекту	К библиотеке
CHGJOBQ	Очередь заданий	*DTAAUT			*READ, *ADD, *DLT, *OBJMGMT	*EXECUTE
		*OWNER			Владелец ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CLRJOBQ ¹	Очереди заданий	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTJOBQ ¹	Очереди заданий					*READ, *ADD
DLTJOBQ	Очереди заданий				*OBJEXIST	*EXECUTE
HLDJOBQ ¹	Очереди заданий	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT ⁵						
RLSJOBQ ¹	Очереди заданий	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ ^{1,3}	Очереди заданий	*DTAAUT			*READ	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQD	Очередь заданий				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

¹ При наличии специальных прав доступа *SPLCTL никакие права доступа к очереди заданий не нужны, однако необходимы права доступа к библиотеке, содержащей эту очередь.

² Необходимо быть владельцем очереди заданий.

³ Если вы передадите на выполнение команду работы со всеми очередями заданий, то будут показаны все очереди заданий из библиотек, по отношению к которым вам предоставлены права доступа *EXECUTE.

⁴ Для просмотра параметров очереди заданий воспользуйтесь API QSPRJOBQ.

⁵ Для выполнения этой команды необходимы специальные права доступа *ALLOBJ или *AUDIT.

Команды расписания заданий

В этой таблице перечислены права доступа, необходимые для команд расписания заданий.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDJOBSCDE	Расписание заданий	*CHANGE	*EXECUTE
	Описание задания ¹	*USE	*EXECUTE
	Очередь заданий ^{1,2}	*READ	*EXECUTE
	Пользовательский профайл	*USE	*EXECUTE
	Очередь сообщений ¹	*USE, *ADD	*EXECUTE
CHGJOBSCDE ³	Расписание заданий	*CHANGE	*EXECUTE
	Описание задания ¹	*USE	*EXECUTE
	Очередь заданий ^{1,2}	*READ	*EXECUTE
	Пользовательский профайл	*USE	*EXECUTE
	Очередь сообщений ¹	*USE, *ADD	*EXECUTE
HLDJOBSCDE ³	Расписание заданий	*CHANGE	*EXECUTE
RLSJOBSCDE ³	Расписание заданий	*CHANGE	*EXECUTE
RMVJOBSCDE ³	Расписание заданий	*CHANGE	*EXECUTE
WRKJOBSCDE ⁴	Расписание заданий	*USE	*EXECUTE
¹ Необходимые права доступа к указанному объекту должны быть и у пользовательского профайла, добавляющего запись, и у пользовательского профайла, от имени которого будет выполняться задание. ² Права доступа к очереди заданий не должны входить в число принятых прав доступа. ³ Если запись была добавлена другим пользователем, то необходимы специальные права доступа *JOBCTL. ⁴ Если запись была добавлена другим пользователем, то для просмотра подробной информации о записи (опция 5 или формат печати *FULL) необходимы специальные права доступа *JOBCTL.			

Команды работы с журналами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с журналами.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке или каталогу
ADDRMTJRN	Исходный журнал	*CHANGE, *OBJMGT	*EXECUTE
	Целевой журнал		*EXEC, *ADD
APYJRNCHG (Q)	Журналы	*USE	*EXECUTE
	Получатели журналов	*USE	*EXECUTE
	Объекты не из IFS, зарегистрированные изменения которых применяются	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD
	Объекты из IFS, зарегистрированные изменения которых применяются	*RW, *OBJMGT	*RX, если указано subtree(*ALL)

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке или каталогу
APYJRNCHGX (Q)	Журналы	*USE	
	Получатели журналов	*USE	
	Файл	*OBJMGT, *CHANGE, *OBJEXIST'	*EXECUTE, *ADD
CHGJRN (Q)	Получатель журнала, если он указан	*OBJMGT, *USE	*EXECUTE
	Подключенный получатель журнала	*OBJMGT, *USE	*EXECUTE
	Журналы	*OBJOPR, *OBJMGT, *UPD	*EXECUTE
	Журнал, если указана опция RCVSIZOPT(*MINFIXLEN).	*OBJOPR, *OBJMGT, *UPD, *OBJALTER	*EXECUTE
CHGJRNA (Q) ¹⁰			
CHGJRNOBJ ⁹	Журнал	*OBJOPR, *OBJMGT	
	Объекты не из IFS	*READ, *OBJMGT	
	Объекты интегрированной файловой системы	*R, *OBJMGT	*X
	Путь к объекту SUBTREE(*ALL)	*RX, *OBJMGT	
	Путь к объекту SUBTREE(*NONE)	*R, *OBJMGT	
CHGRMTJRN	Исходный журнал	*CHANGE, *OBJMGT	*EXECUTE
	Исходный журнал	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Журналы	*USE	*EXECUTE
	Получатели журналов	*USE	*EXECUTE
	Файл	*USE	*EXECUTE
CPYAUDJRNE ⁸	Файл вывода уже существует	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Файл вывода не существует		*EXECUTE, *ADD
CRTJRN	Журналы		*READ, *ADD
	Получатели журналов	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Журналы	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE ⁸			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке или каталогу
DSPJRN ⁶	Журналы	*USE	*EXECUTE
	Журнал, если задан параметр FILE(*ALLFILE), объект не выбран, указанный объект был удален из системы, объект не был связан с журналом, для одного из выбранных кодов журнала указано значение *IGNFILSLT или *IGNOBSLT, указан OBJJID либо журнал является удаленным.	*OBJEXIST, *USE	*EXECUTE
	Получатели журналов	*USE	*EXECUTE
	Объект не из IFS, если он указан	*USE	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
	Объект из IFS, если он указан	*R (возможно и *X, если объект является каталогом и указано SUBTREE(*ALL))	*X
DSPJRMNU ¹			
ENDJRN	Информация приведена в разделе “Команды интегрированной файловой системы” на стр. 415.		
ENDJRNAP	Журналы	*OBJOPR, *OBJMGT	*EXECUTE
	Файл	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNLIB	Журнал	*OBJOPR, *OBJMGT	*EXECUTE
	Библиотека	*OBJOPR, *OBJMGT, *READ	
ENDJRNOBJ	Журналы	*OBJOPR, *OBJMGT	*EXECUTE
	Объект	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPf	Журналы	*OBJOPR, *OBJMGT	*EXECUTE
	Файл	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP ²			
JRNPf ³			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке или каталогу
RCVJRNE	Журналы	*USE	*EXECUTE
	Журнал, если задан параметр FILE(*ALLFILE), объект не выбран, указанный объект был удален из системы, объект не был связан с журналом, для одного из выбранных кодов журнала указано значение *IGNFILSLT или *IGNOBSLT, указан OBJJID либо журнал является удаленным.	*OBJEXIST, *USE	*EXECUTE
	Получатели журналов	*USE	*EXECUTE
	Объект не из IFS, если он указан	*USE	*EXECUTE
	Объект из IFS, если он указан	*R (возможно и *X, если объект является каталогом и указано SUBTREE(*ALL))	*X
	Программа выхода	*EXECUTE	*EXECUTE
RMVJRNCHG (Q)	Журналы	*USE	*EXECUTE
	Получатели журналов	*USE	*EXECUTE
	Объекты не из IFS, зарегистрированные изменения которых удаляются	*OBJMGT, *CHANGE	*EXECUTE
RTVJRNE	Журналы	*USE	*EXECUTE
	Журнал, если задан параметр FILE(*ALLFILE), объект не выбран, указанный объект был удален из системы, объект не был связан с журналом, для одного из выбранных кодов журнала указано значение *IGNFILSLT или *IGNOBSLT, указан OBJJID либо журнал является удаленным.	*OBJEXIST, *USE	*EXECUTE
	Получатели журналов	*USE	*EXECUTE
	Объект не из IFS, если он указан	*USE	*EXECUTE
	Объект из IFS, если он указан	*R (возможно и *X, если объект является каталогом и указано SUBTREE(*ALL))	*X
	Исходный журнал	*CHG, *OBJMGT	
SNDJRNE	Журналы	*OBJOPR, *ADD	*EXECUTE
	Объект не из IFS, если он указан	*OBJOPR	*EXECUTE
	Объект из IFS, если он указан	*R	*X
STRJRN	Информация приведена в разделе “Команды интегрированной файловой системы” на стр. 415.		
STRJRNAP	Журналы	*OBJOPR, *OBJMGT	*EXECUTE
	Файл	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNLIB	Журнал	*OBJOPR, *OBJMGT	*EXECUTE
	Библиотека	*OBJOPR, *OBJMGT, *READ	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке или каталогу
STRJRNP	Журналы	*OBJOPR, *OBJMGT	*EXECUTE
	Файл	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Журналы	*OBJOPR, *OBJMGT	*EXECUTE
	Объект	*OBJOPR, *READ, *OBJMGT	*EXECUTE
WRKJRN ⁴ (Q)	Журналы	*USE	*READ ⁷
	Получатель журнала	*USE	*EXECUTE
WRKJRNA ⁶	Журналы	*OBJOPR и права доступа к данным, отличные от *EXECUTE	*EXECUTE
	Получатель журнала ⁵	*OBJOPR и права доступа к данным, отличные от *EXECUTE	*EXECUTE
<p>¹ См. описание команды WRKJRN (эта команда выполняет те же функции).</p> <p>² См. описание команды STRJRNP.</p> <p>³ См. описание команды STRJRNP.</p> <p>⁴ Для выполнения отдельных функций, вызываемых во время выполнения выбранной операции, необходимы дополнительные права доступа. Например, для восстановления объекта необходимы права на выполнение команды RSTOBJ или RST.</p> <p>⁵ Если выбрана опция удаления получателей, то необходимы права доступа *OBJOPR и *OBJEXIST к получателям журнала.</p> <p>⁶ Для применения параметра JRN(*INTSYSJRN) необходимы специальные права доступа *ALLOBJ.</p> <p>⁷ Для просмотра меню WRKJRN необходимы права на чтение (*READ) библиотеки журнала. Для работы с опцией этого меню необходимы права доступа *EXECUTE к указанной библиотеке.</p> <p>⁸ Для выполнения этой команды необходимы специальные права доступа *AUDIT.</p> <p>⁹ Для применения параметра PTLTNS(*ALWUSE) необходимы специальные права доступа *ALLOBJ.</p> <p>¹⁰ Для выполнения этой команды необходимы специальные права доступа *JOBCTL.</p>			

Команды для работы с получателем журнала

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с получателем журнала.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTJRNRVCV	Получатели журналов		*READ, *ADD
DLTJRNRVCV	Получатели журналов	*OBJOPR, *OBJEXIST и права доступа к данным, отличные от *EXECUTE	*EXECUTE
	Журналы	*OBJOPR	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DSPJRNRCVA	Получатели журналов	*OBJOPR и права доступа к данным, отличные от *EXECUTE	*EXECUTE
	Журнал, если он подключен	*OBJOPR	*EXECUTE
WRKJRNRCV ^{1, 2, 3}	Получатели журналов	Любые права доступа	*USE
<p>¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.</p> <p>² Если выбрана опция удаления получателей, то необходимы права доступа *OBJOPR и *OBJEXIST к получателям журнала.</p> <p>³ Если выбрана опция просмотра описания, то пользователю должны быть предоставлены права доступа *OBJOPR к получателям журнала и права доступа к данным этих получателей, отличные от *EXECUTE.</p>			

Команды для работы с Kerberos

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с Kerberos.

Команда	Объект	Тип объекта	Требуемые права доступа к объекту
ADDKRBKTE	Все каталоги в пути к открываемому файлу таблицы ключей.	*DIR	*X
	Родительский каталог целевого файла таблицы ключей в операции добавления, если файл еще не существует.	*DIR	*WX
	Файл таблицы ключей, если указан список.	*STMF	*R
	Целевой файл таблицы ключей в операциях добавления или удаления.	*STMF	*RW
	Все каталоги в пути к файлам конфигурации.	*DIR	*X
	Файлы конфигурации	*STMF	*R
ADDKRBTKT	Все каталоги в пути к файлу таблицы ключей	*DIR	*X
	Файл таблицы ключей	*STMF	*R
	Все каталоги в пути к файлу кэша идентификационных данных	*DIR	*X
	Файл кэша идентификационных данных	*STMF	*RW
	Родительский каталог файла кэша, если он указан в переменной среды KRB5CCNAME и если файл будет создан	*DIR	*WX
	Все каталоги в пути к файлам конфигурации	*DIR	*X
	Файлы конфигурации	*STMF	*R
CHGKRBPWD			

Команда	Объект	Тип объекта	Требуемые права доступа к объекту
DLTKRBCCF	Все каталоги в пути к файлу кэша идентификационных данных, если этот файл не находится в каталоге по умолчанию.	*DIR	*X
	Родительский каталог в пути к файлу кэша идентификационных данных, если этот файл не находится в каталоге по умолчанию.	*DIR	*WX
	Файл кэша идентификационных данных, если этот файл не находится в каталоге по умолчанию.	*STMF	*RW, *OBJEXIST
	Все каталоги в пути к файлам конфигурации, если файл кэша идентификационных данных не находится в каталоге по умолчанию.	*DIR	*X
	Файлы конфигурации, если файл кэша идентификационных данных не находится в каталоге по умолчанию.	*STMF	*R
DLTKRBCCF	Все каталоги в пути, если файл кэша идентификационных данных находится в каталоге по умолчанию.	*DIR	*X
	Файл кэша идентификационных данных, если этот файл находится в каталоге по умолчанию.	*STMF	*RW
	Все каталоги в пути к файлам конфигурации, если файл кэша идентификационных данных находится в каталоге по умолчанию.	*DIR	*X
	Файлы конфигурации, если файл кэша идентификационных данных находится в каталоге по умолчанию.	*STMF	*R
DSPKRBCCF	Все каталоги в пути к файлу таблицы ключей	*DIR	*X
	Файл таблицы ключей	*STMF	*R
	Все каталоги в пути к файлу кэша идентификационных данных	*DIR	*X
	Файл кэша идентификационных данных	*STMF	*RW
DSPKRBKTE	Все каталоги в пути к открываемому файлу таблицы ключей.	*DIR	*X
	Родительский каталог целевого файла таблицы ключей в операции добавления, если файл еще не существует.	*DIR	*WX
	Файл таблицы ключей, если указан список.	*STMF	*R
	Целевой файл таблицы ключей в операциях добавления или удаления.	*STMF	*RW
	Все каталоги в пути к файлам конфигурации.	*DIR	*X
	Файлы конфигурации	*STMF	*R

Команда	Объект	Тип объекта	Требуемые права доступа к объекту
RMVCRBKTE	Все каталоги в пути к открываемому файлу таблицы ключей.	*DIR	*X
	Родительский каталог целевого файла таблицы ключей в операции добавления, если файл еще не существует.	*DIR	*WX
	Файл таблицы ключей, если указан список.	*STMF	*R
	Целевой файл таблицы ключей в операциях добавления или удаления.	*STMF	*RW
	Все каталоги в пути к файлам конфигурации.	*DIR	*X
	Файлы конфигурации	*STMF	*R

Команды для работы с языками программирования

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с языками программирования.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CLOSE	Команда Закрывать	*USE	*EXECUTE
CRTBNDC	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Каталог, указанный в параметре OUTPUT, PPSRCSTMF или MAKEDEP	*USE	*EXECUTE
	Файл, указанный в параметре OUTPUT, PPSRCSTMF или MAKEDEP	См. общие правила.	*READ, *ADD
CRTBNDCBL	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Каталог связывания	*USE	*EXECUTE
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTBNDCBL	Исходный файл	*USE	*EXECUTE
	Включаемый файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	См. общие правила.
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTBNDCPP	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Каталог, указанный в параметре OUTPUT, PPSRCSTMF, TEMPLATE или MAKEDEP	*USE	*EXECUTE
	Файл, указанный в параметре OUTPUT, PPSRCSTMF, TEMPLATE или MAKEDEP	См. общие правила.	*READ, *ADD
	Заголовки, генерируемые параметром TEMPLATE	*USE	*EXECUTE
CRTBNDRPG	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Каталог связывания	*USE	*EXECUTE
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
	CRTCBMOD	Исходный файл	*USE
Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа		*OBJOPR	*EXECUTE
Модуль: REPLACE(*NO)			*READ, *ADD
Модуль: REPLACE(*YES)		См. общие правила.	*READ, *ADD
Таблица, указанная в параметре SRTSEQ		*USE	*EXECUTE
CRTCLD		Исходный файл	*USE
	Объект локали - REPLACE(*NO)		*READ, *ADD
	Объект локали - REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTCLMOD	Исходный файл	*USE	*EXECUTE
	Включаемый файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	См. общие правила.
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTCLPGM (Создать программу на CL)	Исходный файл	*USE	*EXECUTE
	Включаемый файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	См. общие правила.
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTCVLPGM (лицензионная программа COBOL/400* или среда S/38)	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTCMOD	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Модуль: REPLACE(*NO)		*READ, *ADD
	Модуль: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Файл, указанный в параметре OUTPUT, PPSRCSTMF или MAKEDEP	*USE	*EXECUTE
	Файл, указанный в параметре OUTPUT, PPSRCSTMF или MAKEDEP	См. общие правила.	*READ, *ADD
CRTCPPMOD	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Модуль: REPLACE(*NO)		*READ, *ADD
	Модуль: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Каталог, указанный в параметре OUTPUT, PPSRCSTMF, TEMPLATE или MAKEDEP	*USE	*EXECUTE
	Файл, указанный в параметре OUTPUT, PPSRCSTMF, TEMPLATE или MAKEDEP	См. общие правила.	*READ, *ADD
	Заголовки, генерируемые параметром TEMPLATE	*USE	*EXECUTE
CRTRPGMOD	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Модуль: REPLACE(*NO)		*READ, *ADD
	Модуль: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTRPGPM (лицензионная программа RPG/400* и среда S/38)	Исходный файл	*USE	*EXECUTE
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTRPTPGM (лицензионная программа RPG/400 и среда S/38)	Исходный файл	*USE	*EXECUTE
	Программа - REPLACE(*NO)		*READ, *ADD
	Программа - REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Исходный файл для создаваемой программы RPG	См. общие правила.	См. общие правила.
	Внешне описанные файлы устройств и файлы базы данных, к которым обращается исходная программа	*OBJOPR	*EXECUTE
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTS36CBL (среда S/36)	Исходный файл	*USE	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTS36RPG	Исходный файл	*USE	*READ, *ADD
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа - REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTS36RPGR	Исходный файл	*USE	*READ, *ADD
	Файл дисплея: REPLACE(*NO)		*READ, *ADD
	Файл дисплея: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTS36RPT	Исходный файл	*USE	*EXECUTE
	Исходный файл для создаваемой программы RPG	См. общие правила.	См. общие правила.
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTSQLCI (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Объект: REPLACE(*NO)		*READ, *ADD
	Объект: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTSQLCBL (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTSQLCBLI (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Объект: REPLACE(*NO)		*READ, *ADD
	Объект: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTSQLCPPI (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTSQLFTN (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTSQLPLI (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTSQLRPG (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CRTSQLRPGI (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) 1	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Объект: REPLACE(*NO)		*READ, *ADD
	Объект: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE
CVTRPGSRC	Исходный файл	*USE	*EXECUTE
	Файл вывода	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Файл протокола	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
CVTSQLCPP ¹	Исходный файл	*OBJOPR, *READ	*EXECUTE
	Целевой исходный файл	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Спецификации описания данных	*OBJOPR	*EXECUTE
	Программа: REPLACE(*NO)		*READ, *ADD
	Программа: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Таблица, указанная в параметре SRTSEQ	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ENDCBLDBG (лицензионная программа COBOL/400 или среда S/38)	Программа	*CHANGE	*EXECUTE
ENTCBLDBG (среда S/38)	Программа	*CHANGE	*EXECUTE
DLTCLD	Объект локали	*OBJEXIST, *OBJMGT	*EXECUTE
INCLUDE	Исходный файл	*USE	*EXECUTE
RTVCLDSRC	Объект локали	*USE	*EXECUTE
	Целевой файл	См. общие правила.	См. общие правила.
RUNSQLSTM ¹	Исходный файл	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Программа	*CHANGE	*EXECUTE
STREXPRC	Исходный файл	*USE	*EXECUTE
	Программа выхода	*USE	*EXECUTE
STRSQL (лицензионная программа DB2 Query Manager and SQL Development for i5/OS) ¹	Таблица последовательности сортировки	*USE	*EXECUTE
	Описание принтера	*USE	*EXECUTE
	Очередь вывода на принтер	*USE	*EXECUTE
	Файл принтера	*USE	*EXECUTE
¹ Дополнительная информация о требованиях к защите операторов SQL приведена в разделе Авторизация, права доступа и принадлежность объектов.			

Команды для работы с библиотеками

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с библиотеками.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDLIBLE	Библиотека		*USE
CHGCURLIB	Новая текущая библиотека		*USE
CHGLIB ⁸	Библиотека		*OBJMGT
CHGLIBL	Все библиотеки в списке библиотек		*USE
CHGSYSLIBL (Q)	Библиотеки в новом списке		*USE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CLRLIB ³	Все объекты, удаляемые из библиотеки	*OBJEXIST	*USE
	Объекты типа *DTADCT ¹⁴ , *JRN ¹⁴ , *JRNRCV ¹⁴ , *MSGQ ¹⁴ , *SBSD ¹⁴	Ознакомьтесь с правами доступа, необходимыми для выполнения команды DLTxxx для соответствующего типа объекта	
	ASP (если он указан)	*USE	
CPYLIB ⁴	Исходная библиотека		*USE
	Целевая библиотека, если она существует		*USE, *ADD
	Команды CHKOBJ, CRTDUPOBJ	*USE	
	Команда CRTLIB (если требуется создать целевую библиотеку)	*USE	
	Копируемый объект	Права доступа, необходимые для применения команды CRTDUPOBJ к объекту соответствующего типа.	
CRTLIB ⁹	ASP (если он указан)	*USE	
DLTLIB ³	Все объекты, удаляемые из библиотеки	*OBJEXIST	*USE, *OBJEXIST
	Объекты типа *DTADCT ¹⁴ , *JRN ¹⁴ , *JRNRCV ¹⁴ , *MSGQ, *SBSD ¹⁴	Ознакомьтесь с правами доступа, необходимыми для выполнения команды DLTxxx для соответствующего типа объекта	
	ASP (если он указан)	*USE	
DSPLIB	Библиотека		*READ
	Объекты в библиотеке ⁵	Любые права доступа, отличные от *EXCLUDE	
	ASP (если он указан)	*EXECUTE	
DSPLIBD	Библиотека		Любые права доступа, отличные от *EXCLUDE
EDTLIBL	Библиотека, добавляемая в список		*USE
RCLLIB	Библиотека		*USE, *OBJEXIST

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
I RSTLIB (Q) ^{7, 17, 19}	Определение носителя	*USE	*EXECUTE
	Библиотека, если она существует		*READ, *ADD
	Очереди сообщений, восстанавливаемые в библиотеке, в которой они уже существуют	*OBJOPR, *OBJEXIST ⁷	*EXECUTE, *READ, *ADD
	Программы, принимающие права доступа	Права владельца, либо *ALLOBJ и *SECADM	*EXECUTE
	Сохраненная библиотека, если указан параметр VOL(*SAVVOL)		*USE ⁶
	Все объекты, восстанавливаемые поверх существующих объектов в библиотеке	*OBJEXIST ³	*EXECUTE, *READ, *ADD
	Пользовательский профайл, которому принадлежат создаваемые объекты	*ADD ⁶	
	Лентопротяжное устройство, дисковод, оптический накопитель	*USE	*EXECUTE
	Файл вывода, если он указан	См. общие правила	См. общие правила
	Файл описания полей QSYS/QASAVOBJ, если указан несуществующий файл вывода	*USE	*EXECUTE
RSTLIB (Q)	Файл магнитной ленты (QSYSTAP) или дискеты (QSYSDKT)	*USE ⁶	*EXECUTE
	Вывод на принтер QSYS/QPSRLDSP, если задано OUTPUT(*PRINT)	*USE	*EXECUTE
	Файл сохранения	*USE	*EXECUTE
	Оптический файл (OPTFILE) ¹²	*R	Не применимо
	Префикс пути к оптическому файлу (OPTFILE) ¹²	*X	Не применимо
	Оптический том ¹¹	*USE	
	Описание ASP ¹⁵	*USE	
RSTS36LIBM	Исходный файл	*USE	*EXECUTE
	Целевой файл	*CHANGE	*EXECUTE
	Целевая библиотека	*CHANGE	*EXECUTE
	Файл устройства или описание устройства	*USE	*EXECUTE
RTVLIBD	Библиотека		Любые права доступа, отличные от *EXCLUDE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
SAVLIB ¹⁸	Все объекты в библиотеке	*OBJEXIST ⁶	*READ, *EXECUTE
	Определение носителя	*USE	*EXECUTE
	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE
	Файл сохранения (если в нем есть записи)	*USE, *ADD, *OBJMGT	*EXECUTE
	Очередь сообщений о сохранении активных объектов	*OBJOPR, *ADD	*EXECUTE
	Лентопротяжное устройство, дисковод, оптический накопитель	*USE	*EXECUTE
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Файл описания полей QSYS/QASAVOBJ, если указан несуществующий файл вывода	*USE ⁶	*EXECUTE
	Вывод на принтер QSYS/QPSAVOBJ	*USE ⁶	*EXECUTE
	Пространство пользователя команды, если задано	*USE	*EXECUTE
SAVLIB	Оптический файл ¹²	*RW	Не применимо
	Родительский каталог файла (OPTFILE) ¹²	*WX	Не применимо
	Префикс пути к оптическому файлу (OPTFILE) ¹²	*X	Не применимо
	Корневой каталог (/) оптического тома ^{12, 13}	*RWX	Не применимо
	Оптический том ¹¹	*CHANGE	
	Описание ASP ¹⁵	*USE	
SAVRSTLIB	В исходной системе - те же права доступа, что и для команды SAVLIB.		
	В целевой системе - те же права доступа, что и для команды RSTLIB.		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
SAVS36LIBM	Целевой физический файл	*OBJOPR, *OBJMGT	*EXECUTE
	QSYSDKT для дискеты или QSYSTAR для магнитной ленты; всем командам необходимы права доступа к устройству	*OBJOPR	*EXECUTE
	Целевой физический файл, если указан параметр MBROPT(*ADD)	*ADD	*READ, *ADD
	Целевой физический файл, если указан параметр MBROPT(*REPLACE)	*ADD, *DLT	*EXECUTE
	Исходная библиотека		*USE
WRKLIB ^{10, 16}	Библиотека		*USE
1	В этом столбце указаны права доступа к библиотеке, над которой выполняется действие. Например, для добавления библиотеки CUSTLIB в список библиотек с помощью команды ADDLIBLE необходимы права на использование библиотеки CUSTLIB.		
2	В этом столбце указаны права доступа к библиотеке QSYS, поскольку все библиотеки содержатся в библиотеке QSYS.		
3	Если пользователю не предоставлены права к существованию некоторых объектов библиотеки, то эти объекты не удаляются, а библиотека очищается и удаляется не полностью. Удаляются только те объекты, по отношению к которым пользователю предоставлены права доступа.		
4	Все ограничения, применимые к команде CRTDUPOBJ, также действуют и в отношении данной команды.		
5	Если у вас нет прав доступа к объекту в библиотеке, то для этого объекта будет показано описание *NOT AUTHORIZED.		
6	Если пользователю предоставлены специальные права доступа *SAVSYS, то указанные права доступа не нужны.		
7	Для того чтобы присвоить параметру Разрешить различия в объектах (ALWOBJDIF) значение, отличное от *NONE, необходимы специальные права доступа *ALLOBJ.		
8	Для изменения значения параметра библиотеки CRTOBJAUD необходимы специальные права доступа *AUDIT. Если вы изменяете только значение CRTOBJAUD, права доступа *OBJMGT не требуются. Если помимо CRTOBJAUD вы изменяете и другие значения, то необходимы права доступа *OBJMGT.		
9	Для того чтобы указать значение CRTOBJAUD, отличное от *SYSVAL, необходимы специальные права доступа *AUDIT.		
10	Для выполнения отдельной операции необходимы права на выполнение этой операции.		
11	Оптические тома фактически не являются объектами системы. Связь между оптическим томом и списком прав доступа, применяемым для ограничения доступа к тому, устанавливается функцией поддержки оптической памяти.		
12	Наличие этих прав доступа проверяется только для оптических носителей формата UDF.		
13	Эти права доступа проверяются только при очистке оптического тома.		
14	Данный объект допустим в независимом ASP.		
15	Права доступа необходимы только в том случае, если для выполнения сохранения или восстановления необходимо изменить пространство имен библиотек.		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
16	Для применения этой команды необходимы специальные права доступа *ALLOBJ.		
17	Для указания в параметре PVTAUT значения *YES необходимы специальные права доступа *ALLOBJ.		
18	Для указания в параметре PVTAUT значения *YES необходимы специальные права доступа *ALLOBJ или *SAVSYS.		
19	Для указания имени параметра DFRID необходимы специальные права доступа *SAVSYS.		

Команды для работы с ключами лицензий

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с ключами лицензий.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDLICENSE (Q)	Файл вывода	*USE	*EXECUTE
DSPLICENSE (Q)	Файл вывода	См. общие правила.	См. общие правила.
RMVLICENSE (Q)	Файл вывода	*CHANGE	*EXECUTE

Команды лицензионных программ

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с лицензионными программами.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGLICINF (Q)	Команда WRKICINF	*USE	*EXECUTE
DLTLICPGM ^{1,2} (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM ^{1,2} (Q)			
SAVLICPGM ^{1,2} (Q)			
WRKICINF (Q)			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
¹	Для удаления, сохранения и восстановления некоторых лицензионных программ требуется регистрация в системном каталоге рассылки.		
²	Если выполняется удаление, восстановление или сохранение лицензионной программы, которая содержит папки, то для данной команды действуют те же ограничения, что и для команды DLTDL0.		
³	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		

Команды описания линии

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием линии.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGLINASC ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
	Описание контроллера (SWTCTLLST)	*USE	*EXECUTE
CHGLINBSC ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
	Описание контроллера (SWTCTLLST)	*USE	*EXECUTE
CHGLINDDI ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINETH ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFAX ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFR ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINPPP ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINSDLC ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTDLC ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTRN ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
CHGLINX25 ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
	Описание контроллера (SWTCTLLST)	*USE	*EXECUTE
	Список соединений (CNNLSTIN или CNNLSTOUT)	*USE	*EXECUTE
	Описание сетевого интерфейса (SWTNWILST)	*USE	*EXECUTE
CHGLINWLS ²	Описание линии	*CHANGE, *OBJMGT	*EXECUTE
	Программа (INZPGM)	*USE	*EXECUTE
CRTLINASC ²	Описание контроллера (CTL и SWTCTLLST)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
CRTLINBSC ²	Описание контроллера (SWTCTLLST и CTL)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
CRTLINDDI ²	Описание линии		*READ, *ADD
	Описание сетевого интерфейса (NWI)	*USE	*EXECUTE
	Описание контроллера (NETCTL)	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTLINETH ²	Описание контроллера (NETCTL)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
	Описание сетевого интерфейса (NWI)	*USE	*EXECUTE
	Описание сетевого сервера (NWS)	*USE	*EXECUTE
CRTLINFAX ²	Описание линии		*READ, *ADD
	Описание контроллера	*USE	*EXECUTE
CRTLINFR ²	Описание линии		*READ, *ADD
	Описание сетевого интерфейса (NWI)	*USE	*EXECUTE
	Описание контроллера (NETCTL)	*USE	*EXECUTE
CRTLINPPP ²	Описание контроллера (NETCTL)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
CRTLINS DLC ²	Описание контроллера (CTL)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
CRTLINTDLC ²	Описание контроллера (WSC и CTL)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
CRTLINTRN ²	Описание контроллера (NETCTL)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
	Описание сетевого интерфейса (NWI)	*USE	*EXECUTE
	Описание сетевого сервера (NWS)	*USE	*EXECUTE
CRTLINX25 ²	Описание контроллера (SWTCTLLST)	*USE	*EXECUTE
	Описание контроллера PVC (LGLCHLE)	*USE	*EXECUTE
	Описание линии		*READ, *ADD
	Список соединений (CNNLSTIN или CNNLSTOUT)	*USE	*EXECUTE
	Описание сетевого интерфейса (NWI или SWTNWILST)	*USE	*EXECUTE
CRTLINWLS ²	Описание линии		*READ, *ADD
	Описание контроллера (NETCTL)	*USE	*EXECUTE
	Программа (INZPGM)	*USE	*EXECUTE
DLTLIND	Описание линии	*OBJEXIST	*EXECUTE
DSPLIND	Описание линии	*USE	*EXECUTE
ENDLINRCY	Описание линии	*OBJOPR	*EXECUTE
PRTCMNSEC ^{2, 3}			
RSMLINRCY	Описание линии	*OBJOPR	*EXECUTE
WRKLIND ¹	Описание линии	*OBJOPR	*EXECUTE
¹	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
²	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.		
³	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ.		

Команды для работы в локальной сети (LAN)

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы в локальной сети (LAN).

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам:			
ADDLANADPI CHGLANADPI	DSPLANADPP DSPLANSTS	RMVLANADPT (Q) RMVLANADPI	WRKLANADPT

Команды работы с локалью

В этой таблице перечислены права доступа, необходимые для команд работы с локалью.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTLOCALE	Исходный файл	*USE	*USE, *ADD
DLTLOCALE	Локаль	*OBJEXIST	*EXECUTE

Команды среды почтового сервера

В этой таблице перечислены права доступа, необходимые для выполнения команд среды почтового сервера.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующей команды не требуются никакие права доступа к объектам:			
ENDMSF (Q)	STRMSF (Q)		

Команды для работы с носителями

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с носителями.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDTAPCTG	Описание библиотеки магнитных лент	*USE	*EXECUTE
CFGDEVMLB ¹	Описание библиотеки магнитных лент	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Описание библиотеки магнитных лент	*CHANGE, *OBJMGT	*EXECUTE
CHGJOBMLBA ⁴	Описание библиотеки магнитных лент	*CHANGE	*EXECUTE
CHGTAPCTG	Описание библиотеки магнитных лент	*USE	*EXECUTE
CHKDKT	Описание дисководов	*USE	*EXECUTE
CHKTAP	Описание лентопротяжного устройства	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CLRDKT	Описание дисководов	*USE	*EXECUTE
CRTTAPCGY	Описание библиотеки магнитных лент		
DLTDKTLBL	Описание дисководов	*USE	*EXECUTE
DLTMEDDFN	Определение носителя	*OBJEXIST	*EXECUTE
DLTTAPCGY	Описание библиотеки магнитных лент		
DMPTAP (Q) ⁵	Описание лентопротяжного устройства	*USE	*EXECUTE
DSPDKT	Описание дисководов	*USE	*EXECUTE
DSPTAP	Описание лентопротяжного устройства	*USE	*EXECUTE
DSPTAPCGY	Описание библиотеки магнитных лент		
DSPTAPCTG	Описание библиотеки магнитных лент	*USE	*EXECUTE
DSPTAPSTS	Описание библиотеки магнитных лент	*USE	*EXECUTE
DUPDKT	Описание дисководов	*USE	*EXECUTE
DUPTAP	Описание лентопротяжного устройства	*USE	*EXECUTE
INZDKT	Описание дисководов	*USE	*EXECUTE
INZTAP	Описание лентопротяжного устройства	*USE	*EXECUTE
RMVTAPCTG	Описание библиотеки магнитных лент	*USE	*EXECUTE
RNMDKT	Описание дисководов	*USE	*EXECUTE
SETTAPCGY	Описание библиотеки магнитных лент	*USE	*EXECUTE
WRKMLBRSCQ ³	Описание библиотеки магнитных лент	*USE	*EXECUTE
WRKMLBSTS ² (Q)	Описание библиотеки магнитных лент	*USE	*EXECUTE
WRKTAPCTG	Описание библиотеки магнитных лент	*USE	*EXECUTE
¹	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.		
²	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
³	Для изменения атрибутов библиотеки носителей на время сеанса нужны права доступа *CHANGE к описанию библиотеки магнитных лент. Для изменения приоритета или работы с заданием другого пользователя необходимы специальные права доступа *JOBCTL.		
⁴	Для изменения приоритета или работы с заданием другого пользователя необходимы специальные права доступа *JOBCTL.		
⁵	Для применения этой команды необходимы специальные права доступа *ALLOBJ, когда указано TYPE(*HEX) или для магнитной ленты установлен флаг защиты тома или флаг защиты файла.		

Команды для работы с группами панелей и меню

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с группами панелей и меню.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGMNU	Меню	*CHANGE	*USE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTMNU	Исходный файл	*USE	*EXECUTE
	Меню: REPLACE(*NO)		*READ, *ADD
	Меню: REPLACE(*YES)	См. общие правила.	*READ, *ADD
CRTPNLGRP	Группа панелей: Replace(*NO)		*READ, *ADD
	Группа панелей: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Исходный файл	*USE	*EXECUTE
	Включаемый файл	*USE	*EXECUTE
CRTS36MNU	Меню: REPLACE(*NO)		*READ, *ADD
	Меню: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Исходный файл	*USE	*EXECUTE
	Файлы сообщений, указанные в исходном тексте	*OBJOPR, *OBJEXIST	*EXECUTE
	Исходный файл приемника, если TOMBR не равно *NONE	*OBJOPR, *OBJMGT, *OBJEXIST, *ADD	*READ, *ADD
	Файл меню, если указано REPLACE(*YES)	*OBJOPR, *OBJEXIST	*EXECUTE
	Текстовый файл сообщений команды	*OBJOPR, *OBJEXIST	*EXECUTE
	Команда Создать файл сообщений (CRTMSGF)	*OBJOPR	*EXECUTE
	Команда Добавить описание сообщения (ADDMSGD)	*OBJOPR	*EXECUTE
	Команда Создать файл дисплея (CRTDSPF)	*OBJOPR	*EXECUTE
DLTMNU	Меню	*OBJOPR, *OBJEXIST	*EXECUTE
DLTPNLGRP	Группа панелей	*OBJEXIST	*EXECUTE
DSPMNUA	Меню	*USE	*USE
GO	Меню	*USE	*USE
	Файл меню и файлы сообщений, если указано *DSPF	*USE	*EXECUTE
	Текущая и рабочая библиотеки	*USE	
	Программа, если указано *PGM	*USE	*EXECUTE
WRKMNU ¹	Меню	Любой	*USE
WRKPNLGRP ¹	Группа панелей	Любой	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.			

Команды для работы с сообщениями

В этой таблице перечислены права доступа, необходимые для команд работы с сообщениями.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DSPMSG	Очередь сообщений	*USE	*USE
	Очередь сообщений, принимающая ответ на сообщение-вопрос	*USE, *ADD	*USE
	Удаляемые сообщения из очереди сообщений	*USE, *DLT	*USE
RCVMSG	Очередь сообщений	*USE	*EXECUTE
	Удаляемые сообщения из очереди	*USE, *DLT	*EXECUTE
RMVMSG	Очередь сообщений	*OBJOPR, *DLT	*EXECUTE
RTVMSG	Файл сообщений	*USE	*EXECUTE
SNDBRKMSG	Очередь сообщений, принимающая ответ на сообщения-вопросы	*OBJOPR, *ADD	*EXECUTE
SNDMSG	Очередь сообщений	*OBOPR, *ADD	*EXECUTE
	Очередь сообщений, принимающая ответ на сообщение-вопрос	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Очередь сообщений	*OBJOPR, *ADD	*EXECUTE
	Файл сообщений при отправке предопределенного сообщения	*USE	*EXECUTE
	Очередь сообщений, принимающая ответ на сообщение-вопрос	*OBJOPR, *ADD	*EXECUTE
SNDRPY	Очередь сообщений	*USE, *ADD	*EXECUTE
	Удаляемые сообщения из очереди	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Очередь сообщений	*OBJOPR, *ADD	*EXECUTE
	Файл сообщений при отправке предопределенного сообщения	*USE	*EXECUTE
WRKMSG	Очередь сообщений	*USE	*USE
	Очередь сообщений, принимающая ответ на сообщение-вопрос	*USE, *ADD	*USE
	Удаляемые сообщения из очереди сообщений	*USE, *DLT	*USE

Команды для работы с описанием сообщений

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием сообщений.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDMSGD	Файл сообщений	*USE, *ADD	*EXECUTE
CHGMSGD	Файл сообщений	*USE, *UPD	*EXECUTE
DSPMSGD	Файл сообщений	*USE	*EXECUTE
RMVMSGD	Файл сообщений	*OBJOPR, *DLT	*EXECUTE
WRKMSGD ¹	Файл сообщений	*USE	*EXECUTE

¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.

Команды для работы с файлами сообщений

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с файлами сообщений.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGMSGF	Файл сообщений	*USE, *DLT	*EXECUTE
CRTMSGF	Файл сообщений		*READ, *ADD
DLTMSGF	Файл сообщений	*OBJEXIST	*EXECUTE
DSPMSGF	Файл сообщений	*USE	*EXECUTE
MRGMSGF	Исходный файл сообщений	*USE	*EXECUTE
	Целевой файл сообщений	*USE, *ADD, *DLT	*EXECUTE
	Заменяемый файл сообщений	*USE, *ADD	*EXECUTE
WRKMSGF ¹	Файл сообщений	Любые права доступа	*USE

¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.

Команды для работы с очередью сообщений

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с очередью сообщений.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGMSGQ	Очередь сообщений	*USE, *DLT	*EXECUTE
CLRMSGQ	Очередь сообщений	*OBJOPR, *DLT	*EXECUTE
CRTMSGQ	Очередь сообщений		*READ, *ADD
DLTMSGQ	Очередь сообщений	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPLOG			*EXECUTE
WRKMSGQ ¹	Очередь сообщений	Любые права доступа	*USE

¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.

Команды переноса данных

В этой таблице перечислены права доступа, необходимые для выполнения команд переноса данных.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RCVMGRDTA	Файл	*ALL	*READ, *ADD
	Устройство	*CHANGE	*EXECUTE
SNDMGRDTA	Файл	*ALL	*READ, *ADD
	Устройство	*CHANGE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
<p>Для выполнения следующих команд не требуются никакие права доступа к объектам.</p> <p>Они поставляются с общими правами доступа *EXCLUDE. Для применения этих команд необходимы специальные права доступа *ALLOBJ.</p>			
ANZS34OCL ANZS36OCL CHGS34LIBM CHKS36SRCA CVTBASSTR CVTBASUNF CVTBGUDTA CVTS36FCT	CVTS36JOB CVTS38JOB GENS36RPT GENS38RPT MGRS36 MGRS36APF ¹ MGRS36CBL MGRS36DFU ¹	MGRS36DSPF MGRS36ITM MGRS36LIB MGRS36MNU MGRS36MSGF MGRS36QRY ¹ MGRS36RPG MGRS36SEC MGRS38OBJ	MIGRATE QMUS36 RESMGRNAM RSTS38AUT STRS36MGR STRS38MGR
¹ Необходимы специальные права доступа *ALLOBJ. Должен быть установлен компонент 4 i5/OS.			

Команды описания режима

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием режима.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGMODD ²	Описание режима	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD ²	Описание режима		*READ, *ADD
CHGSSNMAX	Описание устройства	*OBJOPR	*EXECUTE
DLTMODD	Описание режима	*OBJEXIST	*EXECUTE
DSPMODD	Описание режима	*USE	*EXECUTE
DSPMODSTS	Устройство	*OBJOPR	*EXECUTE
	Описание режима	*OBJOPR	*EXECUTE
ENDMOD	Описание устройства	*OBJOPR	*EXECUTE
STRMOD	Описание устройства	*OBJOPR	*EXECUTE
WRKMODD ¹	Описание режима	*OBJOPR	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.			
² Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			

Команды для работы с модулями

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с модулями.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGMOD	Модуль	*OBJMGT, *USE	*USE
	Модуль, если указано OPTIMIZE	*OBJMGT, *USE	*USE, *ADD, *DLT
	Модуль, если указано FRCRRT(*YES)	*OBJMGT, *USE	*USE, *ADD, *DLT
	Модуль, если указано ENBPRFCOL	*OBJMGT, *USE	*USE, *ADD, *DELETE
DLTMOD	Модуль	*OBJEXIST	*EXECUTE
DSPMOD	Модуль	*USE	*EXECUTE
RTVBNDSRC ¹	Модуль	*USE	*EXECUTE
	*SRVPGM и модули, указанные с *SRVPGM	*USE	*EXECUTE
	Исходный файл базы данных, если файл и элемент существуют, и указано MBROPT(*REPLACE).	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Исходный файл базы данных, если файл и элемент существуют, и указано MBROPT(*ADD)	*OBJOPR, *ADD	*EXECUTE
	Исходный файл базы данных, если файл существует, а элемент нужно создать.	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *READ, *ADD
	Исходный файл базы данных, если нужно создать файл и элемент.		*EXECUTE, *READ, *ADD
	Команда CRTSCRPF, если файл не существует		*EXECUTE
	Команда ADDPFM, если элемент не существует		*EXECUTE
	Команда RGZPFM для реорганизации элемента исходного файла	*OBJMGT	*EXECUTE
WRKMOD ²	Модуль	Любые права доступа	*USE
¹	<p>Для выполнения следующих команд необходимы права доступа *USE:</p> <ul style="list-style-type: none"> • CRTSCRPF, если файл не существует. • ADDPFM, если элемент не существует. • RGZPFM для реорганизации элемента исходного файла. Для реорганизации элемента исходного файла нужны права доступа *CHANGE и *OBJALTER, либо права доступа *OBJMGT. В этом случае после выполнения команды RTVBNDSRC элемент исходного файла будет реорганизован так, что все порядковые номера будут равны нулю. 		
²	<p>Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.</p>		

Команды описания NetBIOS

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием NetBIOS.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGNTBD ²	Описание NetBIOS	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD ²	Описание NetBIOS		*EXECUTE
DLTNTBD	Описание NetBIOS	*OBJEXIST	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DSPNTBD	Описание NetBIOS	*USE	*EXECUTE
WKRNTBD ¹	Описание NetBIOS	*OBJOPR	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.			
² Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			

Команды для работы с сетью

В этой таблице перечислены права доступа, необходимые для команд работы с сетью.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDNETJOBE (Q)	Пользовательский профайл в записи сетевого задания	*USE	
APING	Описание устройства	*CHANGE	
AREXEC	Описание устройства	*CHANGE	
CHGNETA (Q) ⁴			
CHGNETJOBE (Q)	Пользовательский профайл в записи сетевого задания	*USE	
DLTNETF ²	Файл вывода	См. общие правила.	См. общие правила.
DSPNETA			
RCVNETF ²	Элемент целевого файла не существует, указано MBROPT(*ADD)	*OBJMGT, *USE	*EXECUTE, *ADD
	Элемент целевого файла не существует, указано MBROPT(*REPLACE)	*OBJMGT, *CHANGE	*EXECUTE, *ADD
	Элемент целевого файла существует, указано MBROPT(*ADD)	*USE	*EXECUTE
	Элемент целевого файла существует, указано MBROPT(*REPLACE)	*OBJMGT, *CHANGE	*EXECUTE
RMVNETJOBE (Q)	Пользовательский профайл в записи сетевого задания	*USE	
RTVNETA			
RUNRMTCMD	Описание устройства	*CHANGE	
SNDNETF	Физический файл или файл сохранения	*USE	*EXECUTE
SNDNETMSG локальному пользователю	Очередь сообщений	*OBJOPR, *ADD	*EXECUTE
VFYAPPCNN	Описание устройства	*CHANGE	
WRKNETF ^{2,3}			
WRKNETJOBE ³	QUSRSYS/QANFNJE	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
¹	Необходимы специальные права доступа *ALLOBJ.		
²	Пользователь может выполнять эти команды для собственных сетевых файлов и сетевых файлов, принадлежащих его группе. Для обработки сетевых файлов других пользователей необходимы специальные права доступа *ALLOBJ.		
³	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
⁴	Для изменения некоторых сетевых атрибутов необходимы специальные права доступа *IOSYSCFG, либо *ALLOBJ и *IOSYSCFG.		

Команды для работы с сетевой файловой системой

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с сетевой файловой системой.

Команда	Объект	Тип объекта	Файловая система	Требуемые права доступа к объекту
ADDMFS ^{1,3}	каталог-монтажирования	*DIR	корневая (/)	*W
CHGNFSEXP ^{1,2}	Префикс пути	См. общие правила.		
DSPMFSINF	некоторые-каталоги	*DIR	корневая (/)	*RX
	Префикс пути	См. общие правила.		
ENDNFSSVR ^{1,4}	нет			
EXPORTFS ^{1,2}	Префикс пути	См. общие правила.		
MOUNT ^{1,3}	каталог-монтажирования	*DIR	корневая (/)	*W
RLSIFSLCK ¹	объекта	*STMF	корневая (/), QOpenSys, UDFS	*R
	Префикс пути	См. общие правила.		
RMVMFS ¹				
STATFS	некоторые-каталоги	*DIR	корневая (/)	*RX
	Префикс пути	См. общие правила.		
STRNFSSVR ¹	нет			
UNMOUNT ¹				
¹	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			
²	Если указан флаг -F, а файл /etc/exports не существует, то необходимы права на запись и выполнение (*WX) по отношению к каталогу /etc. Если указан флаг -F, а файл /etc/exports существует, то необходимы права на чтение и запись по отношению к файлу /etc/exports и права (*X) по отношению к каталогу /etc.			
³	Каталог, в котором выполняется монтажирование - это любой каталог интегрированной файловой системы, в котором необходимо смонтировать файловую систему.			
⁴	Для завершения работы заданий демона, запущенных другим пользователем, необходимы специальные права доступа *JOBCTL.			

Команды для работы с описанием сетевого интерфейса

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием сетевого интерфейса.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGNWIFR ²	Описание сетевого интерфейса	*CHANGE, *OBJMGT	*EXECUTE
CRTNWIFR ²	Описание сетевого интерфейса		*READ, *ADD
	Описание линии связи (DLCI)	*USE	*EXECUTE
DLTNWID	Описание сетевого интерфейса	*OBJEXIST	*EXECUTE
DSPNWID	Описание сетевого интерфейса	*USE	*EXECUTE
WRKNWID ¹	Описание сетевого интерфейса	*OBJOPR	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией. ² Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			

Команды для работы с сетевым сервером

В этой таблице перечислены права доступа, необходимые для команд работы с сетевым сервером.

Команда	Объект	Тип объекта	Файловая система	Требуемые права доступа к объекту
ADDNWSSTGL ²	Путь (/QFPNWSSTG)	*DIR	корневая (/)	*X
	Родительский каталог (имя области памяти)	*DIR	корневая (/)	*WX
	Файлы, составляющие область памяти	*STMF	корневая (/)	*RW
	Описание сетевого сервера	*NWS D	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSSTG ²	Путь (корневой каталог и /QFPNWSSTG)	*DIR	корневая (/)	*WX
CHGNWSUSRA ⁴	Пользовательский профайл	*USRPRF		*OBJMGT, *USE
CRTNWSSTG ²	Путь (корневой каталог и /QFPNWSSTG)	*DIR	корневая (/)	*WX
DLTNWSSTG ²	Путь (/QFPNWSSTG)	*DIR	корневая (/)	*WX
	Родительский каталог (имя области памяти)	*DIR	корневая (/)	*RWX, *OBJEXIST
	Файлы, составляющие область памяти	*STMF	корневая (/)	*OBJEXIST
DLTWNTSVR ⁵	Описание сетевого сервера	*NWS D	QSYS.LIB	*OBJEXIST
	Описание линии	*LIND	QSYS.LIB	*OBJEXIST
	Конфигурация сетевого сервера	*NWS CFG	QSYS.LIB	*OBJEXIST
	Область памяти сетевого сервера - путь (/QFPNWSSTG)	*DIR	корневая (/)	*WX
	Родительский каталог (имя области памяти)	*DIR	корневая (/)	*RWX, *OBJEXIST
	Файлы, составляющие область памяти	*STMF	корневая (/)	*OBJEXIST

Команда	Объект	Тип объекта	Файловая система	Требуемые права доступа к объекту
DSPNWSSTG	Префикс пути	См. общие правила		
	Файлы, составляющие область памяти	*STMF	корневая (/)	*R
INSWNTSVR ^{6,7}	Описание сетевого сервера	*NWS	Не применимо	*USE
	Описание линии	*LIND	Не применимо	*USE
	Конфигурация сетевого сервера	*NWSCFG	Не применимо	*USE
	Область памяти сетевого сервера - путь (/QFPNWSSTG)	*DIR	корневая (/)	*WX
RMVNWSSTGL ²	Путь (/QFPNWSSTG)	*DIR	корневая (/)	*X
	Родительский каталог (имя области памяти)	*DIR	корневая (/)	*WX
	Файлы, составляющие область памяти	*STMF	корневая (/)	*RW
	Описание сетевого сервера	*NWS	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Префикс пути	См. общие правила		
	Файлы, составляющие область памяти	*STMF	корневая (/)	*R
Для выполнения следующих команд не требуются никакие права доступа к объектам:				
ADDRMTSVR CHGNWSA ^{4(Q)} CHGNWSALS CRTNWSALS DLTNWSALS DSPNWSA	DSPNWSALS DSPNWSSN DSPNWSSTC DSPNWSUSRA SBMNWSCMD (Q) ³		SNDNWSMSG WRKNWSALS WRKNWSEN WRKNWSSN WRKNWSSTS	
¹	Принятые права доступа не применяются в командах для работы с сетевым сервером.			
²	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			
³	Для работы с этой командой нужны специальные права доступа *JOBCTL.			
⁴	Для того чтобы присвоить параметрам NDSTREELST и NTW3SVRLST значения, отличные от *NONE, необходимы специальные права доступа *SECADM.			
⁵	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG и *ALLOBJ.			
⁶	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG, *ALLOBJ и *JOBCTL.			
⁷	Для того чтобы присвоить параметрам IPSECRULE, CHAPAUT и SPCERTID значения, отличные от применяемых по умолчанию, необходимы специальные права доступа *SECADM.			

Команды настройки сетевого сервера

В этой таблице перечислены права доступа, необходимые для выполнения команд настройки сетевого сервера.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке QUSRSYS
CHGNWSCFG ^{1,3}	Конфигурация сетевого сервера	*CHANGE	*EXECUTE
CRTNWSCFG ^{1,3}	Конфигурация сетевого сервера	*USE	*READ, *ADD
DLTNWSCFG ^{1,3}	Конфигурация сетевого сервера	*OBJEXIST	*EXECUTE
DSPNWSCFG ^{1,3}	Конфигурация сетевого сервера	*USE	*EXECUTE
INZNWSCFG ^{1,2}	Конфигурация сетевого сервера	*CHANGE	*EXECUTE
WRKNWSCFG ¹	Конфигурация сетевого сервера	*USE	*EXECUTE
<p>¹ Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.</p> <p>² Для выполнения этой команды необходимы специальные права доступа *SECADM.</p> <p>³ Для того чтобы присвоить параметрам IPSECRULE, CHAPAUT и SPCERTID значения, отличные от применяемых по умолчанию, или просмотреть такие значения этих параметров, необходимы специальные права доступа администратора защиты (*SECADM).</p>			

Команды для работы с описанием сетевого сервера

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с описанием сетевого сервера.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке QSYS
CHGNWSD ²	Описание сетевого сервера	*CHANGE, *OBJMGT	*EXECUTE
	Описание NetBIOS (NTB)	*USE	*EXECUTE
CRTNWSD ²	Описание NetBIOS (NTB)	*USE	*EXECUTE
	Описание линии связи (PORTS)	*USE	*EXECUTE
DLTNWSD	Описание сетевого сервера	*OBJEXIST	*EXECUTE
DSPNWSD	Описание сетевого сервера	*USE	*EXECUTE
WRKNWSD ¹	Описание сетевого сервера	*OBJOPR	*EXECUTE
<p>¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.</p> <p>² Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.</p>			

Команды для работы со списком узлов

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы со списком узлов.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDNODLE	Список узлов	*OBJOPR, *ADD	*EXECUTE
CRTNODL	Список узлов		*READ, *ADD

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTNODL	Список узлов	*OBJEXIST	*EXECUTE
RMVNODLE	Список узлов	*OBJOPR, *READ, *DLT	*EXECUTE
WRKNODL ¹	Список узлов	*USE	*USE
WRKNODLE	Список узлов	*USE	*EXECUTE
¹ Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.			

Команды служб Office

В этой таблице перечислены права доступа, необходимые для выполнения команд служб Office.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам.			
ADDACC (Q) DSPACC DSPACCAUT DSPUSRPMN	GRTACCAUT ^{2,3,6} (Q) GRTUSRPMN ^{1,2} RMVACC ¹ (Q) RVKACCAUT ¹	RVKUSRPMN ^{1,2} WRKDOCLIB ⁴ WRKDOCPRQ ⁵	
¹	Для предоставления другим пользователям прав кода доступа или прав доступа к документу, а также для аннулирования таких прав необходимы специальные права доступа *ALLOBJ.		
²	Запрещен доступ ко всем документам, папкам и почтовым сообщениям, кроме личных.		
³	Перед предоставлением прав кода доступа необходимо определить этот код доступа в системе (с помощью команды Добавить код доступа (ADDACC)). Пользователь, получающий права кода доступа, должен быть зарегистрирован в системном каталоге рассылки.		
⁴	Необходимы специальные права доступа *SECADM.		
⁵	Для выполнения некоторых функций, вызываемых при выполнении выбранной операции, необходимы дополнительные права доступа. Кроме того, необходимы права доступа ко всем командам, вызываемым при выполнении операции.		
⁶	Для предоставления другим пользователям прав доступа к коду доступа необходимы специальные права доступа ко всем объектам (*ALLOBJ) или специальные права доступа администратора защиты (*SECADM).		

Команды диалогового обучения

В этой таблице перечислены права доступа, необходимые для выполнения команд диалогового обучения.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CVTEDU			
STREDU			

Команды операционной поддержки

В этой таблице перечислены права доступа, необходимые для выполнения команд операционной поддержки.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGBCKUP ¹	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP ²			
CHGPWRSCD ³			
CHGPWRSCDE ³			
DSPBCKSTS	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUPL	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
DSPPWRSCD			
EDTBCKUPL ¹	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*CHANGE	*EXECUTE
ENDCLNUP ⁴	ENDJOB *CMD	*USE	*EXECUTE
PRTDSKINF (Q)	QUSRSYS/QAEZDISK *FILE, элемент QCURRENT	*USE	*EXECUTE
	ASP (если он указан)	*USE	
RTVBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
RTVCLNUP			
RTVDSKINF (Q) ⁵	ASP (если он указан)	*USE	
RTVPWRSCDE	Команда DSPPWRSCD	*USE	
RUNBCKUP ¹	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
	Команды SAVLIB, SAVCHGOBJ, SAVDLO, SAVSECDTA, SAVCFG, SAVCAL и SAV	*USE	*EXECUTE
STRCLNUP ⁴	Пользовательский профайл QPGMR	*USE	
	Очереди заданий	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
1	Необходимы специальные права доступа *ALLOBJ или *SAVSYS.		
2	Необходимы специальные права доступа *ALLOBJ, *SECADM, и *JOBCTL.		
3	Необходимы специальные права доступа *ALLOBJ и *SECADM.		
4	Необходимы специальные права доступа *JOBCTL.		
5	Необходимы специальные права доступа *ALLOBJ.		

Команды для работы с оптической памятью

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с оптической памятью.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа		
		Объект	Библиотека	Оптический том ¹
ADDOPTCTG (Q)	Оптический накопитель	*USE	*EXECUTE	
ADDOPTSVR (Q)	CSI сервера	*USE	*EXECUTE	
CHGDEVOPT ⁴	Оптический накопитель	*CHANGE, *OBJMGT	*EXECUTE	
CHGOPTA (Q)				
CHGOPTVOL	Корневой каталог (/) тома при изменении текстового описания ⁵	*W	Не применимо	Не применимо
	Оптический накопитель	*USE	*EXECUTE	*CHANGE ³
	CSI сервера	*USE	*EXECUTE	Не применимо
CHKOPTVOL	Оптическое устройство	*USE	*EXECUTE	*USE
	Корневой каталог (/) тома	*RWX	Не применимо	Не применимо
CRYPOT	Оптический накопитель	*USE	*EXECUTE	*USE - Исходный том
				*ALL - Целевой том
	Все предшествующие каталоги в пути к исходному файлу	*X	Не применимо	Не применимо
	Все предшествующие каталоги в пути к целевому файлу	*X	Не применимо	Не применимо
	Исходный файл (*DSTMF) ⁵	*R	Не применимо	Не применимо
	Родительский каталог целевого файла	*WX	Не применимо	Не применимо
	Предок родительского каталога при создании каталога	*WX	Не применимо	Не применимо

Команда	Объект	Необходимые права доступа		
		Объект	Библиотека	Оптический том ¹
CPYOPT	Целевой файл, если он заменен вследствие SLTFILE(*ALL)	*W	Не применимо	Не применимо
	Целевой файл, если он заменен вследствие SLTFILE(*CHANGED)	*RW	Не применимо	Не применимо
	Все предшествующие каталоги в пути к исходному каталогу	*X	Не применимо	Не применимо
	Все предшествующие каталоги в пути к целевому каталогу	*X	Не применимо	Не применимо
CPYOPT	Копируемый каталог ⁵	*R	Не применимо	Не применимо
	Копируемый каталог, если он содержит записи	*RX	Не применимо	Не применимо
	Родительский каталог целевого каталога	*WX	Не применимо	Не применимо
	Целевой каталог, если он заменен вследствие SLTFILE(*ALL)	*W	Не применимо	Не применимо
	Целевой каталог, если он заменен вследствие SLTFILE(*CHANGED)	*RW	Не применимо	Не применимо
	Целевой каталог, если будут созданы записи	*WX	Не применимо	Не применимо
CPYOPT	Исходные файлы	*R	Не применимо	Не применимо
	Целевой файл, если он заменен вследствие SLTFILE(*ALL)	*W	Не применимо	Не применимо
	Целевой файл, если он заменен вследствие SLTFILE(*CHANGED)	*RW	Не применимо	Не применимо
CRTDEVOPT ⁴	Оптический накопитель		*EXECUTE	
CVTOPTVKU	Оптический накопитель	*USE	*EXECUTE	*ALL
DSPOPT	Префикс пути, если задано DATA (*SAVRST) ⁵	*X	Не применимо	Не применимо
	Префикс файла, если задано (*SAVRST) ²	*R	Не применимо	Не применимо
	Оптический накопитель	*EXECUTE	*USE	
	CSI сервера	*USE	*EXECUTE	
DSPOPTLCK				
DSPOPTSVR	CSI сервера	*USE	*EXECUTE	
DUPOPT	Оптический накопитель	*USE	*EXECUTE	*USE - Исходный том
				*ALL - Целевой том

Команда	Объект	Необходимые права доступа		
		Объект	Библиотека	Оптический том ¹
INZOPT	Корневой каталог (/) тома	*RWX	Не применимо	Не применимо
	Оптический накопитель	*USE	*EXECUTE	*ALL
LODOPTFMW	Потоковый файл	*R	Не применимо	Не применимо
	Префикс пути	См. общие правила.		
RCLOPT (Q)	Оптический накопитель	*USE	*EXECUTE	
RMVLOPTCTG (Q)	Оптический накопитель	*USE	*EXECUTE	
RMVOPTSVR (Q)	CSI сервера	*USE	*EXECUTE	
WRKHLDOPTF ²	Оптический накопитель	*USE	*EXECUTE	*USE
	CSI сервера	*USE	*EXECUTE	
WRKOPTDIR ²	Оптический накопитель	*USE	*EXECUTE	*USE
	CSI сервера	*USE	*EXECUTE	
WRKOPTF ²	Оптический накопитель	*USE	*EXECUTE	*USE
	CSI сервера	*USE	*EXECUTE	
WRKOPTVOL ²	Оптический накопитель	*USE	*EXECUTE	

¹ Оптические тома фактически не являются объектами системы. Связь между оптическим томом и списком прав доступа, применяемым для ограничения доступа к тому, устанавливается функцией поддержки оптической памяти.

² В утилитах работы с оптической памятью предусмотрено семь опций, которые не являются командами. Они указаны ниже вместе с необходимыми правами доступа к оптическому тому.

- Удалить файл: *CHANGE
- Переименовать файл: *CHANGE
- Удалить каталог: *CHANGE
- Создать каталог: *CHANGE
- Переименовать том: *ALL
- Разблокировать оптический файл: *CHANGE
- Сохранить заблокированный оптический файл: *USE - исходный том, *Change - Целевой том

³ Для изменения списка прав доступа, применяемого для защиты тома, нужны права доступа на управление списком прав доступа.

⁴ Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.

⁵ Наличие этих прав доступа проверяется только для оптических носителей формата UDF.

Команды очереди вывода

В этой таблице перечислены права доступа, необходимые для выполнения команд очереди вывода.

Команда	Объект	Параметры очереди вывода		Специальные права доступа	Необходимые права доступа	
		AUTCHK	OPRCTL		К объекту	К библиотеке
CHGOUTQ ¹	Очередь данных				*READ	*EXECUTE
	Очереди вывода	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Очередь сообщений				*OBJOPR *ADD	*EXECUTE
	Объект настройки рабочей станции				*USE	*EXECUTE
	Программа преобразования польз. данных				*OBJOPR *EXECUTE	*EXECUTE
	Программа польз. драйвера				*OBJOPR *EXECUTE	*EXECUTE
CLROUTQ ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTOUTQ	Очередь данных				*READ	*EXECUTE
	Очереди вывода					*READ, *ADD
	Очередь сообщений				*OBJOPR *ADD	*EXECUTE
	Объект настройки рабочей станции				*USE	*EXECUTE
DLTOUTQ	Очереди вывода				*OBJEXIST	*EXECUTE
HLDOUTQ ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT ⁴						
RLSOUTQ ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Права владельца ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

Команда	Объект	Параметры очереди вывода		Специальные права доступа	Необходимые права доступа	
		AUTCHK	OPRCTL		К объекту	К библиотеке
WRKOUTQ ^{1,3}	Очереди вывода				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQD ^{1,3}	Очереди вывода				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
¹	При наличии специальных прав доступа *SPLCTL права доступа к очереди вывода не нужны. Однако нужны права доступа *EXECUTE к библиотеке очереди вывода.					
²	Необходимо являться владельцем очереди вывода.					
³	При работе со всеми очередями вывода будут показаны все очереди вывода из библиотек, по отношению к которым пользователю предоставлены права доступа *EXECUTE.					
⁴	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ.					

Команды для работы с пакетами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с пакетами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTSQLPKG	Программа	*OBJOPR, *READ	*EXECUTE
	Пакет SQL: REPLACE(*NO)		*OBJOPR, *READ, *ADD, *EXECUTE
	Пакет SQL: REPLACE(*YES)	*OBJOPR, *OBJMGT, *OBJEXIST, *READ	*OBJOPR, *READ, *ADD, *EXECUTE
DLTSQLPKG	Пакет	*OBJEXIST	*EXECUTE
PRTSQLINF	Пакет	*OBJOPR, *READ	*EXECUTE
	Программа	*OBJOPR, *READ	*EXECUTE
	Служебная программа	*OBJOPR, *READ	*EXECUTE
STRSQL			

Команды для работы со статистикой

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы со статистикой.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставить права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDDWDFN (Q) ⁷			
ADDJWDFN (Q) ⁷			
ADDPDXDFN (Q) ⁵	Библиотека PGM		*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDPEXFTR (Q) ⁵	Библиотека PGMTRG		*EXECUTE
	Библиотека PGMFTR		*EXECUTE
	Путь JVAFTR	*X для каталога	
	Путь PATHFTR	*X для каталога	
ANZBESTMDL (Q) ⁴	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Библиотеки приложения, которые содержат файлы базы данных для анализа		*EXECUTE
	Описание задания	*USE	*EXECUTE
ANZCMDPFR (Q)	Командный файл	*USE	*EXECUTE
	Файл вывода	*USE	*EXECUTE, *ADD
ANZDBF (Q) ⁴	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Описание задания	*USE	*EXECUTE
ANZDBFKEY (Q)	QPFR/QPTANZKC *PGM	*USE	*EXECUTE
	Библиотеки приложения, которые содержат программы для анализа		*EXECUTE
	Описание задания	*USE	*EXECUTE
ANZPGM (Q)	QPFR/QPTANZPC *PGM	*USE	*EXECUTE
	База данных статистики ²		*ADD, *READ
ANZPFRDTA (Q) ⁴	QPFR/QACVPP *PGM	*USE	*EXECUTE
	База данных статистики ²		*ADD, *READ
ANZPFRDT2 (Q) ⁴	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	QAPTAGP *FILE	*CHANGE	*EXECUTE
	Команда DLFCNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
CFGPFRCOL (Q)	Библиотека набора данных		*EXECUTE
CHGFCNARA (Q)	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
CHGGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE	*CHANGE	*EXECUTE
	QAPGGPHF *FILE	*USE	*EXECUTE
CHGGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE	*CHANGE	*EXECUTE
CHGJOBTP (Q)	QPFR/QPTCHGJT *PGM	*USE	*EXECUTE
CHGMGTCOL	MGTCOL	*OBJMGT	
	Пользовательская библиотека		*EXECUTE
CHGPEXDFN (Q) ⁵	Библиотека PGM		*EXECUTE
CHKPFRCOL (Q)			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CPYFCNARA (Q) ⁴	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE в исходной библиотеке	*USE	*EXECUTE
	Целевая библиотека (если QAPGGPHF *FILE не существует)		*EXECUTE, *ADD
	QAPGGPHF *FILE в целевой библиотеке (при добавлении нового графического формата или замене существующего)	*CHANGE	*EXECUTE
CPYGRPHFMT (Q) ⁴	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE в исходной библиотеке	*USE	*EXECUTE
	Целевая библиотека (если QAPGPKGF *FILE не существует)		*EXECUTE, *ADD
	QAPGPKGF *FILE в целевой библиотеке (при добавлении нового графического пакета или замене существующего)	*CHANGE	*EXECUTE
	QAPGGPHF *FILE в целевой библиотеке (при добавлении нового графического пакета или замене существующего)	*USE	*EXECUTE
CPYGRHPKG (Q)	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	Исходная библиотека		*EXECUTE
	Целевая библиотека		*EXECUTE, *ADD
	Описание задания	*USE	*EXECUTE
CPYPRCOL (Q)	Исходная библиотека		*EXECUTE
	Целевая библиотека		*EXECUTE, *ADD
CPYPRDTA (Q)	QPFR/QITCPYCP *PGM	*USE	*EXECUTE
	База данных статистики (все файлы QAPM*)	*USE	*EXECUTE
	Библиотека модели		*EXECUTE, *ADD
	Описание задания	*USE	*EXECUTE
	QPFR/QCYCBMCP *PGM	*USE	*EXECUTE
	QPFR/QCYCBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYOPDBS *PGM	*USE	*EXECUTE
	QPFR/QCYCLIDS *PGM	*USE	*EXECUTE
CRTBESTMDL (Q)	QPFR/QCYCAPT *PGM	*USE	*EXECUTE
	Библиотека, в которой создается функциональная область		*EXECUTE, *ADD
	QARTAPGR *FILE в целевой библиотеке (при добавлении новой функциональной области)	*CHANGE	*EXECUTE
CRTFCNARA (Q)	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	Библиотека, в которой создается графический формат		*EXECUTE, *ADD
	QAPGGPHF *FILE в целевой библиотеке (при добавлении нового графического формата)	*CHANGE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	Библиотека, в которой создается графический пакет		*EXECUTE, *ADD
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
	QAPGPKGF *FILE в целевой библиотеке (при добавлении нового графического пакета)	*USE	*EXECUTE
CRTGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	Библиотека, в которой создаются данные хронологии		*ADD, *READ
	Описание задания	*USE	*EXECUTE
CRTHSTDTA (Q)	QPFR/QPGCRTHS *PGM	*USE	*EXECUTE
	Целевая библиотека		*ADD, *READ
CRTPEXDTA (Q) ⁵	Библиотека *MGTCOL		*EXECUTE
	Библиотека данных ¹		*READ, *ADD ²
CRTPFRTDTA (Q)	Исходная библиотека		*EXECUTE
	Целевая библиотека		*ADD, *READ
	Исходная библиотека		*USE
CRTPFRSUM (Q)	Пользовательская библиотека		*ADD, *READ
CVTPFCOL (Q)	Исходная библиотека		*USE
	Целевая библиотека		*USE, *ADD
CVTPFRDTA (Q)	Описание задания	*USE	*EXECUTE
CVTPFRTHD (Q)	База данных статистики ²		*ADD, *READ
	Библиотека модели		*EXECUTE, *ADD
	QPFR/QCYDBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYCVTBD *CMD	*USE	*EXECUTE
DLTBESTMDL (Q) ⁴	QPFR/QCYCBTOD *PGM	*USE	*EXECUTE
	QAPTAGP *FILE в библиотеке функциональной области	*CHANGE	*EXECUTE
DLTFCNARA (Q) ⁴	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE в библиотеке графического формата	*CHANGE	*EXECUTE
DLTGPHFMT (Q) ⁴	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE в библиотеке графического пакета	*CHANGE	*EXECUTE
DLTGPHPKG (Q) ⁴	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGHSTD *FILE в библиотеке данных хронологии	*CHANGE	*EXECUTE
	QAPGHSTI *FILE в библиотеке данных хронологии	*CHANGE	*EXECUTE
	QAPGSUMD *FILE в библиотеке данных хронологии	*CHANGE	*EXECUTE
DLTHSTDTA (Q) ⁴	QPFR/QPGDLTHS *PGM	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTPREXDTA (Q) ⁵	Библиотека данных ¹		*EXECUTE, *DELETE ²
DLTPFCOL (Q)	Библиотека		*EXECUTE
DLTPFRDTA (Q) ⁴	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPMEMINF	Файл вывода	См. общие правила	См. общие правила
DMPTRC (Q) ⁵	Библиотека для хранения данных трассировки		*EXECUTE, *ADD
	Файл вывода (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPHSTGPH (Q) ⁴	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Библиотека данных хронологии		*EXECUTE
DSPPFRDTA (Q) ⁴	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	Библиотека формата или пакета		*EXECUTE
	База данных статистики ²		*EXECUTE
	Библиотека файла вывода		*EXECUTE, *ADD
	Очередь вывода	*USE	*EXECUTE
	Описание задания	*USE	*EXECUTE
DSPPFRGPH (Q) ⁴	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Библиотека файла вывода		*EXECUTE
	Описание задания	*USE	*EXECUTE
ENDDW (Q) ⁷			
ENDJOBTRC (Q) ⁴	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDJW (Q) ⁷			
ENDPEX (Q) ⁵	Библиотека данных ¹		*READ, *ADD ²
ENDPFCOL (Q)			
PRTACTRPT (Q) ⁴	QPFR/QITPRTAC *PGM	*USE	*EXECUTE
	База данных статистики ²	*USE	*ADD, *READ
	Описание задания	*USE	*EXECUTE
PRTCPTRPT (Q) ⁴	QPFR/QPTCPTRP *PGM	*USE	*EXECUTE
	База данных статистики ²		*ADD, *READ
	Описание задания	*USE	*EXECUTE
PRTJOBTRPT (Q) ⁴	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	База данных статистики ²		*ADD, *READ
	Описание задания	*USE	*EXECUTE
PRTJOBTRC (Q) ⁴	QPFR/QPTTRCRP *PGM	*USE	*EXECUTE
	Библиотека с файлом трассировки задания (QAPTTRCJ)		*EXECUTE
	Описание задания	*USE	*EXECUTE
PRTLCKRPT (Q) ⁴	QPFR/QPTLCKQ *PGM	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
PRTPEXRPT ⁵	Библиотека данных ¹		*EXECUTE ²
	Файл вывода	*USE	*EXECUTE, *ADD
	QPFR/QVPEPRTC *PGM	*USE	*EXECUTE
	QPFR/QVPESVGN *SRVPGM	*USE	*EXECUTE
	QPFR/QYPESVGN *SRVPGM	*USE	*EXECUTE
PRTPOLRPT (Q) ⁴	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	База данных статистики ²		*ADD, *READ
	Описание задания	*USE	*EXECUTE
PRTRSCRPT (Q) ⁴	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	База данных статистики ²		*ADD, *READ
	Описание задания	*USE	*EXECUTE
PRTSYSRPT (Q) ⁴	QPFR/QPTNSRP *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE		*EXECUTE
	Описание задания	*USE	*EXECUTE
PRTTNSRPT (Q) ⁴	QPFR/QPTNSRP *PGM	*USE	*EXECUTE
	Библиотека файла трассировки (QTRJOBТ)		*EXECUTE
	Описание задания	*USE	*EXECUTE
PRTTRCRPT (Q) ⁴	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE
RMVDWDFN (Q) ⁷			
RMVJWDFN (Q) ⁷			
RMVPEXDFN (Q) ⁵			
RMVPEXFTR (Q) ⁵			
RSTPFCOL (Q)	Библиотека, связанная с восстановлением набора	*EXECUTE,, *ADD ⁶	
	Файл сохранения	*USE	*EXECUTE
SAVPFCOL (Q)	Библиотека, содержащая сохраняемый набор	*EXECUTE ⁶	
	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE, *ADD
	Файл сохранения (если в нем есть записи)	*OBJMGT, *USE, *ADD	*EXECUTE
STRBEST (Q) ⁴	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON ^{3,4}	Файл вывода	*OBJOPR, *ADD	*EXECUTE
STRDW (Q) ⁷	Пользовательская библиотека		*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRJW (Q) ⁷	Пользовательская библиотека		*EXECUTE
STRPEX (Q) ⁵			
STRPFCOL (Q)			
STRPFRG (Q) ⁴	QPFR/QPGSTART *PGM	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRPFRT (Q) ⁴	QPFR/QMNMAIN0 *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE в библиотеке функциональных областей	*CHANGE	*EXECUTE
	Команда CHGFCNARA (Q)	*USE	*EXECUTE
	Команда CPYFCNARA (Q)	*USE	*EXECUTE
	Команда CRTFCNARA (Q)	*USE	*EXECUTE
	Команда DLTFNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
WRKFCNARA (Q) ⁴	QPFR/QPTAGRPC *PGM	*USE	*EXECUTE
	Файл вывода (QAITMON)	*CHANGE, *ALTER	*EXECUTE, *ADD
WRKPEXDFN (Q) ⁵			
WRKPEXFTR (Q) ⁵			
WRKSYSACT (Q) ^{3,4}	QPFR/QITMONCP *PGM	*USE	*EXECUTE
<p>Для выполнения следующих команд не требуются никакие права доступа к объектам:</p> <ul style="list-style-type: none"> • ENDDBMON³ • ENDPFRTRC (Q) • STRPFRTTRC (Q) 			
1	Если указана библиотека по умолчанию (QPEXDATA), то права доступа к этой библиотеке не проверяются.		
2	Пользователю должны быть предоставлены права доступа к библиотеке, содержащей набор файлов базы данных. Права доступа к отдельным наборам файлов базы данных не проверяются.		
3	Для работы с этой командой нужны специальные права доступа *JOBCTL.		
4	Для работы с этой командой нужны специальные права доступа *SERVICE.		
5	Для применения этой команды у вас должны быть специальные права доступа *SERVICE или права доступа к функции Служебная трассировка i5/OS, предоставленные с помощью функции Администрирование приложений System i Navigator. Список пользователей, которым разрешено выполнять операции трассировки, также можно изменить с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав ИД функции QIBM_SERVICE_TRACE.		
6	Если пользователю предоставлены специальные права доступа *SAVSYS, то указанные права доступа не нужны.		
7	Для применения этой команды у вас должны быть специальные права на обслуживание (*SERVICE) или права доступа к функции операционной системы Наблюдение за диском посредством функции Администрирование приложений System i Navigator. Список пользователей, которым разрешено выполнять инструмент наблюдения за диском, также можно изменить с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав ИД функции QIBM_SERVICE_DISK_WATCHER.		

Команды для работы с группой дескрипторов печати

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с группой дескрипторов печати.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGPDGPRF	Пользовательский профайл	*OBJMGT	
CRTPDG	Группа дескрипторов печати		*READ, *ADD
DLTPDG	Группа дескрипторов печати	*OBJEXIST	*EXECUTE
DSPPDGPRF	Пользовательский профайл	*OBJMGT	
RTVDPGPRF	Пользовательский профайл	*READ	

Команды настройки Print Services Facility

В этой таблице перечислены права доступа, необходимые для выполнения команд настройки Print services facility.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGPSFCFG ^{1,2}			
CRTGPSFCFG ^{1,2}			*READ, *ADD
DLTPSFCFG ^{1,2}	Конфигурация PSF	*OBJEXIST	*EXECUTE
DSPPSFCFG ¹	Конфигурация PSF	*USE	*EXECUTE
WRKPSFCFG ¹	Конфигурация PSF	*READ	*EXECUTE
¹	Для применения этой команды требуется функция PSF/400.		
²	Для применения этой команды нужны специальные права доступа *IOSYSCFG.		

Команды для работы с неполадками

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с неполадками.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDPRBACNE (Q)	Фильтрация	*USE, *ADD	*EXECUTE
ADDPRBSLTE (Q)	Фильтрация	*USE, *ADD	*EXECUTE
ANZPRB (Q)	Команда SNDSRVRQS	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Фильтрация	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Фильтрация	*USE, *UPD	*EXECUTE
DLTPRB (Q) ³	Команда: DLTAPARDTA	*USE	*EXECUTE
DSPPRB	Файл вывода	См. общие правила.	См. общие правила.
PTRINTDTA (Q)			
QRYPRBSTS (Q)			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
VFYCMN (Q)	Описание линии связи ¹	*USE	*EXECUTE
	Описание контроллера ¹	*USE	*EXECUTE
	ИД сети ¹	*USE	*EXECUTE
VFYOPT (Q)	Описание устройства	*USE	*EXECUTE
VFYTP4 (Q)	Описание устройства	*USE, *OBJMGT	*EXECUTE
VFYPRT (Q)	Описание устройства	*USE	*EXECUTE
WRKPRB (Q) ²	Линия, контроллер, NWID (ИД сети) и устройство, полученные в результате анализа неполадки	*USE	*EXECUTE
<p>¹ Необходимы права доступа *USE к проверяемому объекту средств связи.</p> <p>² Для создания отчета о неполадке необходимы права доступа *USE к команде SNDSRVRQS.</p> <p>³ Для того чтобы дополнительно удалить связанные с неполадкой данные APAR, необходимы права доступа к команде DLTAPARDTA. Набор этих прав доступа указан в строке DLTAPARDTA таблицы Службные команды-Необходимые права доступа.</p> <p>⁴ Если описание устройства размещено библиотекой носителей, то необходимы специальные права доступа *IOSYSCFG.</p>			

Команды для работы с программами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы программами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
Права доступа к объектам, необходимые для применения команд CRTxxxPGM, указаны в таблице Языки в разделе “Команды для работы с языками программирования” на стр. 450.			
ADDBKP ¹	Программа обработки точки прерывания	*USE	*EXECUTE
ADDPGM ^{1,2}	Программа	*CHANGE	*EXECUTE
ADDTRC ¹	Программа обработки трассировки	*USE	*EXECUTE
CALL	Программа	*OBJOPR, *EXECUTE	*EXECUTE
	Службная программа ⁴	*EXECUTE	*EXECUTE
CHGDBG	Операция отладки	*USE, *ADD, *DLT	*EXECUTE
CHGHLLPTR ¹			
CHGPGM	Программа	*OBJMGT, *USE	*USE
	Программа, если указана опция повторного создания, изменен уровень оптимизации или изменен набор данных статистики.	*OBJMGT, *USE	*USE, *ADD, *DLT
	Программа, если изменен параметр USRPRF или USEADPAUT	Владелец ⁷	*USE, *ADD, *DLT
CHGPGMVAR ¹			
CHGPTR ¹			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGSRVPGM	Служебная программа	*OBJMGT, *USE	*USE
	Служебная программа, если указана опция повторного создания, изменен уровень оптимизации или изменен набор данных статистики.	*OBJMGT, *USE	*USE, *ADD, *DLT
	Служебная программа, если изменен параметр USRPRF или USEADPAUT.	Владелец ⁷ , *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA ¹			
CRTPGM	Программа, Replace(*NO)	См. общие правила.	*READ, *ADD
	Программа, Replace(*YES)	См. общие правила.	*READ, *ADD
	Служебная программа, указанная в параметре BNDSRVPGM.	*USE	*EXECUTE
	Модуль	*USE	*EXECUTE
	Каталог связывания	*USE	*EXECUTE
CRTSRVPGM	Служебная программа, Replace(*NO)	См. общие правила.	*READ, *ADD
	Служебная программа, Replace(*YES)	См. общие правила.	*READ, *ADD
	Модуль	*USE	*EXECUTE
	Служебная программа, указанная в параметре BNDSRVPGM	*USE	*EXECUTE
	Исходный файл экспорта	*OBJOPR *READ	*EXECUTE
	Каталог связывания	*USE	*EXECUTE
CVTCLSRC	Исходный файл	*USE	*EXECUTE
	Целевой файл	*OBJOPR, *OBJMGT, *USE, *ADD, *DLT	*READ, *ADD
DLTDFUPGM	Программа	*OBJEXIST	*EXECUTE
	Файл дисплея	*OBJEXIST	*EXECUTE
DLTPGM	Программа	*OBJEXIST	*EXECUTE
DLTSRVPGM	Служебная программа	*OBJEXIST	*EXECUTE
DMPCLPGM	Программа на CL	*USE	Нет ³
DSPBKP ¹			
DSPDBG ¹			
DSPDBGWCH			
DSPMODSRC ^{2,4}	Исходный файл	*USE	*USE
	Любые включаемые файлы	*USE	*USE
	Программа	*CHANGE	*EXECUTE
DSPPGM	Программа	*READ	*EXECUTE
	Программа, если указано DETAIL(*MODULE)	*USE	*EXECUTE
DSPPGMREF	Программа	*OBJOPR	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
DSPPGMVAR ¹			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DSPSRVPGM	Служебная программа	*READ	*EXECUTE
	Служебная программа, если указано DETAIL(*MODULE)	*USE	*EXECUTE
DSPTRC ¹			
DSPTRCDTA ¹			
ENDCBLDBG (лицензионная программа COBOL/400 или среда S/38)	Программа	*CHANGE	*EXECUTE
ENDDBG ¹	Программа отладки исходного кода	*USE	*USE
ENDRQS ¹			*EXECUTE
ENTCBLDBG (среда S/38)	Программа	*CHANGE	*EXECUTE
EXTPGMINF	Исходный файл и файлы базы данных	*OBJOPR	*EXECUTE
	Информация о программе		*READ, *ADD
PRTCMDUSG	Программа	*USE	*EXECUTE
RMVBKP ¹			
RMVPGM ¹			
RMVTRC ¹			
RSMBKP ¹			
RTVCLSRC	Программа	*OBJMGT, *USE	*EXECUTE
	Исходный файл базы данных	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SETATNPGM	программа обработки клавиши Attention	*EXECUTE	*EXECUTE
SETPGMINF	Файлы баз данных	*OBJOPR	*EXECUTE
	Исходный файл	*USE	*EXECUTE
	Корневая программа	*CHANGE	*READ, *ADD
	Подпрограмма	*USE	*EXECUTE
STRCBLDBG	Программа	*CHANGE	*EXECUTE
STRDBG	Программа ²	*CHANGE	*EXECUTE
	Исходный файл ⁴	*USE	*EXECUTE
	Любые включаемые файлы ⁴	*USE	*EXECUTE
	Программа отладки исходного кода	*USE	*EXECUTE
	Неотслеживаемая программа сообщений	*USE	*EXECUTE
TFRCTL ⁴	Программа	*USE или права доступа к данным, отличные от *EXECUTE	*EXECUTE
	Некоторые функции языка при использовании языков высокого уровня	*READ	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
UPDPPGM	Программа	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Служебная программа, указанная в параметре BNDSRVPGM.	*USE	*EXECUTE
	Модуль	*USE	*EXECUTE
	Каталог связывания	*USE	*EXECUTE
UPDSRVPGM	Служебная программа	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Служебная программа, указанная в параметре BNDSRVPGM	*USE	*EXECUTE
	Модуль	*USE	*EXECUTE
	Каталог связывания	*USE	*EXECUTE
	Исходный файл экспорта	*OBJOPR *READ	*EXECUTE
WRKPPGM ⁶	Программа	Любые права доступа	*USE
WRKSRVPGM ⁶	Служебная программа	Любые права доступа	*USE
¹	Если для программы уже запущена отладка, то для применения команд отладки никаких дополнительных прав доступа не требуется.		
²	При наличии специальных прав доступа *SERVICE необходимы только права доступа *USE к программе.		
³	Команда DMPCLPGM вызывается из запущенной программы на CL. Поскольку права доступа к библиотеке программы проверяются во время вызова программы, они не будут проверяться при запуске команды DMPCLPGM.		
⁴	Относится только к программам ILE.		
⁵	Дополнительная информация о требованиях к защите операторов SQL приведена в разделе Авторизация, права доступа и принадлежность объектов.		
⁶	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
⁷	Нужно быть владельцем программы или иметь специальные права доступа *ALLOBJ и *SECADM.		

Команды интерпретатора оболочки QSH

В этой таблице перечислены права доступа, необходимые для выполнения команд интерпретатора оболочки QSH.

Для выполнения команд, перечисленных в следующей таблице, не требуются никакие права доступа к объектам.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRQSH ^{1,2}			
QSH ^{1,2}			
¹	QSH - это псевдоним команды CL STRQSH.		
²	Необходимы права доступа *RX ко всем сценариям и права доступа *X ко всем каталогам в пути к сценарию.		

Команды для работы с запросами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с запросами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ANZQRY	Определение запроса	*USE	*EXECUTE
CHGQRYA ⁴			
CRTQMFORM	Форма управления запросами: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Форма управления запросами: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Исходный файл	*USE	*EXECUTE
CRTQMQR	Запрос на управление запросом: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Запрос на управление запросом: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Исходный файл	*USE	*EXECUTE
	Команда OVRDBF	*USE	*EXECUTE
DLTQMFORM	Форма управления запросами	OBJEXIST	*EXECUTE
DLTQMQR	Запрос на управление запросом	*OBJEXIST	*EXECUTE
DLTQRY	Определение запроса	*OBJEXIST	*EXECUTE
RTVQMFORM	Форма Query Manager	*OBJEXIST	*EXECUTE
	Целевой исходный файл	*ALL	*READ, *ADD, *EXECUTE
	Команды ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RTVQMQR	Запрос Query Manager	*USE	*EXECUTE
	Целевой исходный файл	*ALL	*READ, *ADD
	Команды ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RUNQRY	Определение запроса	*USE	*USE
	Файлы ввода	*USE	*EXECUTE
	Файлы вывода	См. общие правила.	См. общие правила.
STRQMQR ¹	Запрос на управление запросом	*USE	*EXECUTE
	Форма управления запросами, если указана	*USE	*EXECUTE
	Определение запроса, если указано	*USE	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
	Команды ADDPFM, CHGOBJD, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTF RMVM (если указано OUTPUT(*OUTFILE))	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRQMPCRC ¹	Исходный файл, содержащий процедуру Query Manager	*USE	*EXECUTE
	Исходный файл, содержащий исходный файл команды, если указан	*USE	*EXECUTE
	Команда OVRPRTF, если результатом действия операторов служит напечатанный отчет или объект запроса.	*USE	*EXECUTE
STRQRY			*EXECUTE
WRKQMFORM ³	Форма управления запросами	Любые права доступа	*USE
WRKQMORY ³	Запрос на управление запросом	Любые права доступа	*USE
WRKQRY ³			
¹	Для выполнения команды STRQM нужны права доступа, необходимые операторам запроса. Например, для того чтобы вставить строку в таблицу, нужны права доступа *OBJOPR, *ADD и *EXECUTE к таблице.		
²	Необходимо быть владельцем объекта или иметь какие-либо права доступа к объекту.		
³	Для выполнения отдельной операции необходимы права доступа, запрашиваемые операцией.		
⁴	Для работы с отдельной командой нужны специальные права доступа *JOBCTL.		

Команды для работы с вопросами и ответами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с вопросами и ответами.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ANSQST (Q)	Файл базы данных QAQAxxBQPY ¹	*READ	*READ
ASKQST	Файл базы данных QAQAxxBBPY ¹ или QAQAxxBQPY ¹	*READ	*READ
CHGQSTDB (Q)	Файл базы данных QAQAxxBQPY ¹	*READ	*READ
CRTQSTDB ² (Q)	Файлы баз данных		*READ, *ADD, *EXECUTE
CRTQSTLOD (Q)	Файл базы данных QAQAxxBQPY ¹	*READ	*READ
DLTQST (Q)	Файл базы данных QAQAxxBQPY ¹	*READ	*READ
DLTQSTDB (Q)	Файл базы данных QAQAxxBQPY ¹	*READ	*READ
EDTQST (Q)	Файл базы данных QAQAxxBQPY ¹	*READ	*READ
LODQSTDB ² (Q)	Файл базы данных QAQAxxBQPY ^{1,3}	*READ	*READ, *ADD, *EXECUTE
STRQST ⁴	Файл базы данных QAQAxxBBPY ¹ или QAQAxxBQPY ¹	*READ	*READ
WRKQST	Файл базы данных QAQAxxBBPY ¹ или QAQAxxBQPY ¹	*READ	*USE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
WRKCNTINF			*EXECUTE
1	“хх” в имени файла - это индекс базы данных вопросов и ответов, с которой работает программа. Индекс представляет собой двузначное число в диапазоне от 00 до 99. Получить индекс базы данных вопросов и ответов можно с помощью команды WRKCNTINF.		
2	Владельцем создаваемых файлов становится профайл пользователя, запустившего команду, если значение параметра OWNER в этом профайле не равно *GRPPRF. Для всех новых файлов, кроме QAQAxxBPPY, устанавливаются общие права доступа *EXCLUDE. Для QAQAxxBPPY устанавливаются Общие права доступа *READ.		
3	Права доступа к файлу необходимы только при загрузке существующей базы данных вопросов и ответов.		
4	Команда показывает меню вопросов и ответов. Для применения опций этого меню необходимы те права доступа, которые запрашиваются выбранной опцией.		

Команды для работы с программой чтения

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с программой чтения.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRDBRDR	Очередь сообщений	*OBJOPR, *ADD	*EXECUTE
	Файл базы данных	*OBJOPR, *USE	*EXECUTE
	Очереди заданий	*READ	*EXECUTE
STRDKTRDR	Очередь сообщений	*OBJOPR, *ADD	*EXECUTE
	Очереди заданий	*READ	*EXECUTE
	Описание устройства	*OBJOPR, *READ	*EXECUTE
Для выполнения следующих команд не требуются никакие права доступа к объектам:			
ENDRDR ¹	HLEDRDR ¹	RLSRDR ¹	
1	Эту операцию разрешено выполнять только пользователю, запустившему программу чтения, а также пользователям со специальными правами доступа ко всем объектам (*ALLOBJ) или правами на управление заданиями (*JOBCTL).		

Команды средства регистрации

В этой таблице перечислены права доступа, необходимые для выполнения команд для средства регистрации.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

Команды для работы с реляционной базой данных

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с реляционной базой данных.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDRDBDIRE	Файл вывода, если он указан	*EXECUTE	*EXECUTE
CHGRDBDIRE	Файл вывода, если он указан	*EXECUTE	*EXECUTE
	Описание устройства из удаленного расположения ⁷	*CHANGE	
DSPRDBDIRE	Файл вывода, если он указан	См. общие правила.	См. общие правила.
Для выполнения следующих команд не требуются никакие права доступа к объектам:			
RMVRDBDIRE WRKRDBDIRE			
¹ Права доступа, проверенные во время использования записи каталога RDB.			

Команды для работы с ресурсами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с ресурсами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DSPHDWRSC			
DSPSFWRSC	Файл вывода, если он указан	См. общие правила.	См. общие правила.
EDTDEVRSC			
WRKHDWRSC ¹			
¹ Для применения опции создания объекта конфигурации необходимы права на использование соответствующей команды CRT.			

Команды для работы с записью удаленного задания (RJE)

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с записью удаленного задания (RJE).

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDFCTE	Таблица управления формами	*DELETE, *USE, *ADD	*READ, *EXECUTE
	Файл устройства ^{1,2}	*USE	*READ, *EXECUTE
	Физический файл ^{1,2} (RJE создает элементы)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Физический файл ^{1,2} (элемент указан)	*USE, *ADD	*READ, *EXECUTE
	Программа ^{1,2}	*USE	*READ, *EXECUTE
	Очередь сообщений ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	QUSER, пользовательский профайл	*USE	*READ, *EXECUTE
ADDRJECMNE	Описание сеанса	*USE, *ADD, *DLT	*READ, *EXECUTE
	Файл BSC/CMN ^{1,2}	*USE	*READ, *EXECUTE
	Описание устройства ²	*USE	*READ, *EXECUTE
	QUSER, пользовательский профайл	*USE	*READ, *EXECUTE
ADDRJERDRE	Описание сеанса	*READ, *ADD, *DLT	*READ, *EXECUTE
	Очередь заданий ²	*READ	*READ, *EXECUTE
	Очередь сообщений ²	*READ, *ADD	*READ, *EXECUTE
ADDRJEW TRE	Описание сеанса	*READ, *ADD, *DLT	*READ, *EXECUTE
	Файл устройства ^{1,2}	*USE	*READ, *EXECUTE
	Физический файл ^{1,2} (RJE создает элементы)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Физический файл ^{1,2} (элемент указан)	*OBJOPR, *ADD	*READ, *EXECUTE
	Программа ^{1,2}	*USE	*READ, *EXECUTE
	Очередь сообщений ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	QUSER, пользовательский профайл	*USE	*READ, *EXECUTE
CHGFCT	Таблица управления формами	*OBJOPR, *OBJMGT	*READ, *EXECUTE
CHGFCTE	Таблица управления формами	*USE	*READ, *EXECUTE
	Файл устройства ^{1,2}	*USE	*READ, *EXECUTE
	Физический файл ^{1,2} (RJE создает элементы)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Физический файл ^{1,2} (элемент указан)	*USE, *ADD	*READ, *EXECUTE
	Программа ^{1,2}	*USE	*READ, *EXECUTE
	Очередь сообщений ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	QUSER, пользовательский профайл	*USE	*READ, *EXECUTE
CHGRJECMNE	Описание сеанса	*USE	*READ, *EXECUTE
	Файл BSC/CMN ^{1,2}	*USE	*READ, *EXECUTE
	Описание устройства ²	*USE	*READ, *EXECUTE
	QUSER, пользовательский профайл	*USE	*READ, *EXECUTE
CHGRJERDRE	Описание сеанса	*USE, *ADD, *DLT	*READ, *EXECUTE
	Очередь заданий ²	*USE	*READ, *EXECUTE
	Очередь сообщений ²	*USE, *ADD	*READ, *EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGRJEWTR	Описание сеанса	*USE	*READ, *EXECUTE
	Файл устройства ^{1,2}	*USE	*READ, *EXECUTE
	Физический файл ^{1,2} (RJE создает элементы)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Физический файл ^{1,2} (элемент указан)	*OBJOPR, *ADD	*READ, *EXECUTE
	Программа ^{1,2}	*USE	*READ, *EXECUTE
	Очередь сообщений ^{1,2}	*USE, *ADD	*READ, *EXECUTE
	QUSER, пользовательский профайл	*USE	*READ, *EXECUTE
CHGSSND	Описание сеанса	*OBJMGT, *READ, *UPD, *OBJOPR	*EXECUTE, *READ
	Очередь заданий ^{1,2}	*USE	*EXECUTE
	Очередь сообщений ^{1,2}	*USE, *ADD	*EXECUTE
	Таблица управления формами ^{1,2}	*USE	*EXECUTE
	QUSER, пользовательский профайл	*USE	*EXECUTE
CNLRJERDR	Описание сеанса	*USE	*EXECUTE
	Очередь сообщений	*USE, *ADD	*EXECUTE
CNLRJEWTR	Описание сеанса	*USE	*EXECUTE
	Очередь сообщений	*USE, *ADD	*EXECUTE
CRTFCT	Таблица управления формами		*READ, *ADD
CRTRJEBSCF	Файл BSC		*READ, *EXECUTE, *ADD
	Исходный физический файл (DDS)	*READ	*EXECUTE
	Описание устройства	*READ	*EXECUTE
CRTRJECFG	Описание сеанса		*READ, *ADD, *UPD, *OBJOPR
	Очереди заданий		*READ, *ADD
	Описание задания		*READ, *OBJOPR, *ADD
	Описание подсистемы		*READ, *OBJOPR, *ADD
	Очередь сообщений		*READ, *ADD
	Файл CMN		*READ, *EXECUTE, *ADD
	Файл BSC		*READ, *EXECUTE, *ADD
	Файл принтера		*USE, *ADD

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTRJECFG	Физический файл		*EXECUTE, *ADD
	Пользовательский профайл ³	*USE	*EXECUTE
	Очереди вывода	*READ	*EXECUTE
	Таблица управления формами	*READ	*READ
	Описание устройства		*EXECUTE
	Описание контроллера		*EXECUTE
	Описание линии		*EXECUTE
CRTRJECMNF	Файл связи		*READ, *EXECUTE, *ADD
	Исходный физический файл (DDS)	*READ	*EXECUTE
	Описание устройства	*READ	*EXECUTE
CRTSSND	Описание сеанса		*READ, *ADD, *UPD, *OBJOPR
	Очередь заданий ^{1,2}	*USE	*EXECUTE
	Очередь сообщений ^{1,2}	*USE, *ADD	*EXECUTE
	Таблица управления формами ^{1,2}	*USE	*EXECUTE
	QUSER, пользовательский профайл	*USE	*EXECUTE
CVTRJEDTA	Таблица управления формами	*USE	*EXECUTE
	Файл ввода	*USE, *UPD	*EXECUTE
	Файл вывода (RJE создает элемент)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Файл вывода (элемент указан)	*USE, *ADD	*EXECUTE
DLTFCT	Таблица управления формами	*OBJEXIST	*EXECUTE
DLTRJECFG	Описание сеанса	*OBJEXIST	*EXECUTE
	Очереди заданий	*OBJEXIST	*EXECUTE
	Файл BSC/CMN	*OBJEXIST, *OBJOPR	*EXECUTE
	Физический файл	*OBJEXIST, *OBJOPR	*EXECUTE
	Файл принтера	*OBJEXIST, OBJOPR	*EXECUTE
	Очередь сообщений	*OBJEXIST, *USE, *DLT	*EXECUTE
	Описание задания	*OBJEXIST	*EXECUTE
	Описание подсистемы	*OBJEXIST, *USE	*EXECUTE
	Описание устройства ⁴	*OBJEXIST	*EXECUTE
	Описание контроллера ⁴	*OBJEXIST	*EXECUTE
	Описание линии ⁴	*OBJEXIST	*EXECUTE
DLTSSND	Описание сеанса	*OBJEXIST	*EXECUTE
DSRJEFCFG	Описание сеанса	*READ	*EXECUTE
ENDRJESSN ⁵	Описание сеанса	*USE	*EXECUTE
RMVFCTE	Таблица управления формами	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RMVRJECMNE	Описание сеанса	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJERDRE	Описание сеанса	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJEWTR	Описание сеанса	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
SNDRJECMD	Описание сеанса	*USE	*EXECUTE
SBMRJEJOB	Описание сеанса	*USE	*EXECUTE
	Файл ввода ⁶	*USE	*EXECUTE
	Очередь сообщений	*USE, *ADD	*EXECUTE
	Объекты, связанные с заданием ⁷		
SNDRJECMD	Описание сеанса	*USE	*EXECUTE
STRRJECSL	Описание сеанса	*USE	*EXECUTE
	Очередь сообщений	*USE	*EXECUTE
STRRJERDR	Описание сеанса	*USE	*USE
STRRJESSN ⁵	Описание сеанса	*USE	*USE, *ADD
	Программа	*USE	*EXECUTE
	Пользовательский профайл QUSER	*USE	*EXECUTE
	Объекты, связанные с заданием ⁷		*EXECUTE
STRRJEWTR	Описание сеанса	*USE	*USE
	Программа ¹	*USE	*READ, *EXECUTE
	Файл устройства ¹	*USE, *ADD	*READ, *EXECUTE
	Физический файл ¹ (RJE создает элементы)	*OBJMGT, *USE, *ADD	*OBJOPR, *ADD
	Физический файл ¹ (элемент указан)	*READ, *ADD	*READ, *EXECUTE
	Очередь сообщений ¹	*USE, *ADD	*READ, *EXECUTE
	QUSER, пользовательский профайл	*USE	*READ, *EXECUTE
WRKFCT ⁸	Таблица управления формами	*USE	*EXECUTE
WRKRJESSN ⁸	Описание сеанса	*USE	*EXECUTE
WRKSSND ⁸	Описание сеанса	*CHANGE	*EXECUTE
¹ Пользовательскому профайлу QUSER необходимы права доступа к этому объекту. ² Если объект не найден или нет необходимых прав доступа, то будет отправлено информационное сообщение, а функция команды продолжит выполнение. ³ Эти права доступа нужны для того, чтобы создать описание задания QRJESSN. ⁴ Эти права доступа нужны только в том случае, если указано DLTCMN(*YES). ⁵ Необходимы специальные права доступа *JOBCTL. ⁶ Файлы ввода содержат файлы, включаемые с помощью элемента .. READFILE. ⁷ Ознакомьтесь с правами доступа, необходимыми для выполнения команды SBMJOB. ⁸ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.			

Команды для работы с атрибутами защиты

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с атрибутами защиты.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGSECA ¹			
CHGSECAUD ^{2,3}			
CFGSYSSEC ^{1,2,3}			
DSPSECA			
DSPSECAUD ³			
PRTSYSSECA ⁴			
¹	Для применения этой команды необходимы специальные права доступа *SECADM.		
²	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ.		
³	Для выполнения этой команды необходимы специальные права доступа *AUDIT.		
⁴	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ или *AUDIT.		

Команды для работы с записью идентификации сервера

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с записью идентификации сервера.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDSVRAUTE ¹			
CHGSVRAUTE ¹			
DSPSVRAUTE	Пользовательский профайл	*READ	*EXECUTE
RMVSVRAUTE ¹			
¹	Если тип пользовательского профайла данной операции отличается от *CURRENT и профайла текущего пользователя задания, то для применения команды необходимы специальные права доступа *SECADM, а также права доступа к профайлу *OBJMGT и *USE.		

Служебные команды

В этой таблице перечислены права доступа, необходимые для выполнения служебных команд.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDTRCFTR ¹¹			
APYPTF (Q)	Библиотека продукта	*OBJMGT	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGSRVA ³ (Q)			
CHKCMNTRC ³ (Q)			*EXECUTE
CHKPRDOPT (Q)	Все объекты компонента продукта ⁴		
CPYPTF ² (Q)	Исходный файл	*USE	*EXECUTE
	Целевой файл ⁸	Те же требования, что и для команды SAVOBJ	Те же требования, что и для команды SAVOBJ
	Описание устройства	*USE	*EXECUTE
	Лицензионная программа		*USE
	Команды: CHKТАР, CPYFRMTAP, CPYTOTAP, CRTLIB, CRTSAVF, CRTTAPF и OVRTAPF	*USE	*EXECUTE
	Библиотека QSRV	*USE	*EXECUTE
CPYPTFGRP ² (Q)	Описание устройства	*USE	*EXECUTE
	Целевой файл	*Те же требования, что и для команды SAVOBJ	*Те же требования, что и для команды SAVOBJ
	Исходный файл	*USE	*EXECUTE
	Команды: CHKТАР, CRTLIB, CRTSAVF	*USE	*EXECUTE
DLTAPARDTA (Q)			
DLTCMNTRC ³ (Q)	NWID (ИД сети) или описание линии	*USE	*EXECUTE
DLTPTF (Q)	Файл сопроводительного письма ⁴		*EXECUTE
	Файл сохранения PTF ⁴		*EXECUTE
DLTRC (Q)	Команда RMVM	*USE	
	Библиотека QSYS	*EXECUTE	
	Файлы базы данных	*OBJEXIST, *OBJOPR	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPTF (Q)	Файл вывода	См. общие правила.	См. общие правила.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
DSPSSTUSR ²⁰			
ENDCMNTRC ³ (Q)	NWID или описание линии	*USE	*EXECUTE
ENDCPYSCN (Q)	Описание устройства	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	Библиотека QSYS	*ADD, *EXECUTE	
	Файлы баз данных	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Команды: PTRTRC, DLTRC	*USE	
EDNWCH ¹⁶ (Q)	Сеансы слежения, контролирующее появление определенного сообщения в протоколе задания ¹⁸		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
INSPTF ⁹ (Q)			
LODPTF (Q)	Описание устройства	*USE	*EXECUTE
LODRUN ²	Команда RSTOBJ	*USE	*EXECUTE
PRTCMNTRC ³ (Q)	NWID (ИД сети) или описание линии	*USE	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
PRTERLOG (Q)	Файл вывода	См. общие правила.	См. общие правила.
PRTINTDTA ^{12,13} (Q)			
PRTTRC ¹¹ (Q)	Библиотека QSYS	*EXECUTE	
	Файлы базы данных	*USE	
	Команда DLTTRC	*USE	
RMVPTF (Q)	Библиотека продукта	*OBJMGT	
RMVTRCFTR ¹¹			
RUNLPDA (Q)	Описание линии	*READ	*EXECUTE
SAVAPARDTA ⁶ (Q)	Команды: CRTDUPOBJ, CRTLIB, CRTOUTQ, CRTSAVF, DLTF, DMPOBJ, DMPSYSOBJ, DSPCTLD, DSPDEV, DSPHWRSC, DSPJOB, DSPLIND, DSPLOG, DSPNWID, DSPPTF, DSPSFWRSC, OVRPRTF, PRTERLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB и WRKSYSVAL	*USE	*EXECUTE
	Существующая неполадка ⁷	*CHANGE	*EXECUTE
SNDPTFORD ¹⁰ (Q)	CRTIMGCLG	*USE	
	QUSRSYS		*ADD, *READ
SNDSRVRS (Q)			
STRCMNTRC ¹¹ (Q)	NWID (ИД сети) или описание линии	*USE	*EXECUTE
	Отслеживаемое задание ¹⁷		
	Программа трассировки	*OBJOPR и *EXECUTE	*EXECUTE
	Очередь сообщений	*USE	*USE
STRCPYSCN	Очереди заданий	*USE	*EXECUTE
	Описание устройства	*USE	*EXECUTE
	Файл вывода, если он указан	См. общие правила.	См. общие правила.
STRSRVJOB (Q)	Пользовательский профайл или задание	*USE	*EXECUTE
STRSST ³ (Q)			
STRTRC (Q) ^{11, 15}	Отслеживаемое задание ¹⁷		
	Программа трассировки	*OBJOPR и *EXECUTE	*EXECUTE
	Очередь сообщений	*USE	*USE
STRWCH ¹⁶ (Q)	Отслеживаемое задание ¹⁷		
	Программа слежения	*OBJOPR и *EXECUTE	*EXECUTE
	Очередь сообщений	*USE	*USE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
TRCCNN ¹¹ (Q)	Отслеживаемое задание ¹⁷		
	Программа трассировки	*OBJOPR и *EXECUTE	*EXECUTE
	Очередь сообщений	*USE	*USE
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT ¹¹ (Q)	Отслеживаемое задание ¹⁷		
	Программа трассировки	*OBJOPR и *EXECUTE	*EXECUTE
	Очередь сообщений	*USE	*USE
TRCJOB (Q)	Файл вывода, если он указан	См. общие правила.	См. общие правила.
	Программа выхода, если она задана	*USE	*EXECUTE
TRCTCPAPP ¹¹ (Q)	Описание линии	*USE	
	Сетевой интерфейс	*USE	
	Сетевой интерфейс	*USE	
	Отслеживаемое задание ¹⁷		
	Программа трассировки	*OBJOPR и *EXECUTE	*EXECUTE
	Очередь сообщений	*USE	*USE
VFYCMN (Q)	Описание линии ⁵	*USE	*EXECUTE
	Описание контроллера ⁵	*USE	*EXECUTE
	ИД сети ⁵	*USE	*EXECUTE
VFYLNKLPDA (Q)	Описание линии	*READ	*EXECUTE
VFYPRT (Q)	Описание устройства	*USE	*EXECUTE
VFYOPT (Q)	Описание устройства	*USE	*EXECUTE
VFYTAP ¹⁴ (Q)	Описание устройства	*USE, *OBJMGT	*EXECUTE
WRKCNTINF (Q)			
WRKFSTAF (Q)	QUSRSYS/QPVINDEX *USRIDX	*CHANGE	*USE
WRKFSTPCT (Q)	QUSRSYS/QVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB ^{1, 10} (Q)	Линия, контроллер, NWID (ИД сети) и устройство, полученные в результате анализа неполадки	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKPTFORD (Q)	QESCPTFO и SNDPTFORD	*USE	
WRKSRVPVD (Q)			
WRKTRC ¹¹ (Q)			
WRKWCH ¹⁹ (Q)			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
1	Для выполнения некоторых процедур анализа неполадки и сохранения записей протокола ошибок необходимы права доступа к команде PRTERLOG.		
2	Также действуют все ограничения для команды RSTOBJ.		
3	Для использования этой команды необходимо иметь специальные права доступа *SERVICE.		
4	Перечисленные объекты используются командой, но права доступа к этим объектам не проверяются. Для применения этих объектов необходимы права доступа к команде.		
5	Необходимы права доступа *USE к проверяемому объекту связи.		
6	Для сохранения буферного файла необходимы специальные права доступа *SPLCTL.		
7	Если команда SAVAPARDTA запускается для новой неполадки, то для этой неполадки создается отдельная библиотека APAR. При повторном запуске команды SAVAPARDTA для сбора дополнительной информации о неполадке пользователю потребуются права доступа к библиотеке APAR этой неполадки.		
8	Опция добавления нового элемента в существующий файл вывода не поддерживается этой командой.		
9	Для данной команды необходимы те же права доступа и действуют те же ограничения, что и для команд APYPTF и LODPTF.		
10	Для применения опций 1 и 3 меню Выбрать способ сообщения необходимы права доступа *USE к команде SNDSRVQRQS. Для параметра IMGDIR установлены следующие ограничения: <ul style="list-style-type: none"> • Необходимы права доступа *X к каждому каталогу пути. • Необходимы права доступа *WX к каталогу, содержащему оптический образ. 		
11	Для применения этой команды у вас должны быть специальные права доступа *SERVICE или права доступа к функции Служебная трассировка i5/OS, предоставленные с помощью функции Администрирование приложений Навигатора System i. Изменить список пользователей, которым предоставлены права на выполнение операций трассировки, можно с помощью команды Изменить права доступа к функции (CHGFCNUSG) с ИД функции QIBM_SERVICE_TRACE.		
12	Для применения этой команды у вас должны быть специальные права доступа *SERVICE или права доступа к функции Служебный дамп i5/OS, предоставленные с помощью функции Администрирование приложений Навигатора System i. Изменить список пользователей, которые могут создавать служебный дамп, можно и с помощью команды Изменить права доступа к функции (CHGFCNUSG) с ИД функции QIBM_SERVICE_DUMP.		
13	Эту команду необходимо запускать в задании или с пользовательским профайлом задания, для которого выполняется печать внутренних данных, либо с пользовательским профайлом, обладающим специальными правами доступа на управление заданиями (*JOBCTL).		
14	Если описание устройства размещено библиотекой носителей, то необходимы специальные права доступа *IOSYSCFG.		
15	Если вы указали шаблон имени пользователя в параметре Имя задания (JOB), то вам необходимы специальные права доступа ко всем объектам (*ALLOBJ) или права доступа к функции Трассировка любого пользователя i5/OS, предоставленные с помощью функции Администрирование приложений Навигатора System i. Список пользователей, которым разрешено выполнять операции трассировки, также можно изменить с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав ИД функции QIBM_ALLOBJ_TRACE_ANY_USER.		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
16	Для применения этой команды у вас должны быть специальные права на обслуживание (*SERVICE) или права доступа к функции i5/OS Службное слежение, предоставленные с помощью функции Администрирование приложений Навигатора System i. Список пользователей, которым разрешено выполнять запускать и завершать операции слежения, также можно изменить с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав ИД функции QIBM_SERVICE_WATCH.		
17	Если задание выполняется под управлением другого пользователя, нежели пользователь отслеживаемого задания, то необходимы специальные права на управление заданием (*JOBCTL). Если в качестве имени отслеживаемого задания указано *ALL или если задан шаблон имени пользователя, то необходимы специальные права доступа ко всем объектам (*ALLOBJ). Пользователь, не имеющий специальных прав доступа *ALLOBJ, может выполнять эту функцию, если у него есть права доступа к функции i5/OS Отслеживать любое задание, предоставленные с помощью функции Администрирование приложений Навигатора System i. Список пользователей, которым разрешено выполнять запускать и завершать операции слежения, также можно изменить с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав ИД функции QIBM_WATCH_ANY_JOB.		
18	Для выполнения команды STRWCH необходимы те же права доступа.		
19	Для применения этой команды у вас должны быть специальные права на обслуживание (*SERVICE) или права доступа к функции i5/OS Службная трассировка и Службное слежение, предоставленные с помощью функции Администрирование приложений Навигатора System i. Список пользователей, которым разрешено выполнять операции трассировки, также можно изменить с помощью команды Изменить права доступа к функции (CHGFCNUSG), указав ИД функции QIBM_SERVICE_TRACE и QIBM_SERVICE_WATCH.		
20	Для выполнения этой команды необходимы права доступа администратора защиты (*AUDIT) и специальные права на контроль (*SECADM).		

Команды для работы с орфографическим словарем

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с орфографическим словарем.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTSPADCT	Орфографический словарь	*OBJEXIST	*EXECUTE
	Словарь - REPLACE(*NO)		*READ, *ADD
	Словарь - REPLACE(*YES)	См. общие правила.	*READ, *ADD
DLTSPADCT	Орфографический словарь	*OBJEXIST	*EXECUTE
WRKSPADCT ¹	Орфографический словарь	Любые права доступа	*USE
¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.			

Команды для работы с сферой управления

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с сферой управления.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDSOCE	Сфера управления ¹	*USE, *ADD	*EXECUTE
DSPSOCSTS			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
RMVSOCE	Сфера управления ¹	*USE, *DLT	*EXECUTE
WRKSOC	Сфера управления ¹	*USE	*EXECUTE

¹ Сфера управления - это физический файл QUSRSYS/QAALSOC.

Команды буферного файла

В этой таблице перечислены права доступа, необходимые для выполнения команд буферного файла.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Параметры очереди вывода			Специальные права доступа	Необходимые права доступа		
		DSPDTA	AUTCHK	OPRCTL		К объекту	К библиотеке	
CHGSPLFA ^{1,2}	Очередь вывода ³		*DTAAUT			*READ, *DLT, *ADD		
			*OWNER			Владелец ⁴		
				*YES	*JOBCTL			
CHGSPLFA ¹ (при перемещении буферного файла)	Исходная очередь вывода ³		*DTAAUT			*READ, *ADD, *DLT		
			*OWNER			Владелец ⁴		
				*YES	*JOBCTL			
	Буферный файл	*OWNER				Владелец ⁶		
	Целевая очередь вывода ⁷			*YES	*JOBCTL	*READ	*EXECUTE	
Целевое устройство					*USE			
CPYSPLF ¹	Файл базы данных					См. общие правила для операции Показать (DSP) или другой операции, использующей файл вывода (OUTPUT (*OUTFILE))	См. общие правила для операции Показать (DSP) или другой операции, использующей файл вывода (OUTPUT (*OUTFILE))	
		Буферный файл	*OWNER			Владелец ⁶		
		Очередь вывода ³	*YES				*READ	
			*NO	*DTAAUT			*READ, *ADD, *DLT	
			*NO	*OWNER			Владелец ⁴	
*YES или *NO		*YES	*JOBCTL					

Команда	Объект	Параметры очереди вывода			Специальные права доступа	Необходимые права доступа	
		DSPDTA	AUTCHK	OPRCTL		К объекту	К библиотеке
DLTEXPSPLF (Q) ¹⁰	Независимый пул дисков ⁹					*USE	
DLTSPLF ¹	Очередь вывода ³		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Владелец ⁴	
				*YES	*JOBCTL		
DSPSPLF ¹	Очередь вывода ³	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Владелец ⁴	
		*YES или *NO		*YES	*JOBCTL		
	Буферный файл	*OWNER				Владелец ⁶	
HLDSPLF ¹	Очередь вывода ³		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Владелец ⁴	
				*YES	*JOBCTL		
RCLSPLSTG (Q) ¹⁰	Независимый пул дисков ⁹					*USE	
RLSSPLF ^{1,8}	Очередь вывода ³		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Владелец ⁴	
				*YES	*JOBCTL		
SNDNETSPLF ^{1,5}	Очередь вывода ³	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Владелец ⁴	
		*YES или *NO		*YES	*JOBCTL		
	Буферный файл	*OWNER				Владелец ⁶	
SNDTCPSPLF ^{1,5}	Очередь вывода ³	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Владелец ⁴	
		*YES или *NO		*YES	*JOBCTL		
	Буферный файл	*OWNER				Владелец ⁶	
STRSPLRCL (Q) ^{9,10}	Независимый пул дисков ⁹					*USE	
WRKSPLF							

Команда	Объект	Параметры очереди вывода			Специальные права доступа	Необходимые права доступа	
		DSPDТА	AUTCHK	OPRCTL		К объекту	К библиотеке
1	У всех пользователей есть права на управление своими буферными файлами.						
2	Для перемещения буферного файла в начало очереди вывода (PRTSEQ(*NEXT)) или настройки его приоритета, превосходящего указанное в пользовательском профайле ограничение, необходимы любые из указанных прав доступа к очереди вывода или специальные права доступа *SPLCTL.						
3	Если у вас есть специальные права доступа *SPLCTL, то указанные права доступа к очереди вывода не нужны.						
4	Необходимо являться владельцем очереди вывода.						
5	Для отправки файла пользователю той же системы необходимы права доступа *USE к очереди вывода и библиотеке очереди вывода получателя.						
6	Пользователь должен быть владельцем буферного файла.						
7	При наличии специальных прав доступа *SPLCTL никакие права доступа к очереди вывода не нужны, однако необходимы права доступа *EXECUTE к библиотеке этой очереди.						
8	Если буферный файл был заблокирован с помощью команды HLDJOB SPLFILE(*YES) и отключен от задания, то у пользователю должны быть права доступа *USE к команде RLSJOB, а также специальные права доступа *JOBCTL или права владельца буферного файла.						
9	Необходимы права доступа *USE для всех независимых пулов дисков в группе независимых пулов дисков.						
10	Для выполнения этой команды необходимы специальные права доступа *SPLCTL.						

Команды для работы с описанием подсистемы

В этой таблице перечислены права доступа, необходимые для выполнения команд с для работы с описанием подсистемы.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDAJE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
	Пользовательский профайл	*USE	
ADDJOBQE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDPJE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Пользовательский профайл	*USE	
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDWSE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
CHGAJE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
	Пользовательский профайл	*USE	
CHGJOBQE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGPJE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Пользовательский профайл	*USE	
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD ^{5, 7}	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Файл меню входа в систему ⁴	*USE	*EXECUTE
CHGWSE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Описание задания ⁹	*OBJOPR, *READ	*EXECUTE
CRTSBSD ^{5 (Q)}	Описание подсистемы		*READ, *ADD
	Файл меню входа в систему ⁴	*USE	*EXECUTE
	Описание устройства ASP ⁸	*USE	
DLTSBSD	Описание подсистемы	*OBJEXIST, *USE	*EXECUTE
DSPSBSD	Описание подсистемы	*OBJOPR, *READ	*EXECUTE
ENDSBS ¹			
PRTSBSDAUT ⁶			
RMVAJE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVCMNE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVJOBQE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVPJE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVRTGE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVWSE	Описание подсистемы	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRSBS ¹	Описание подсистемы	*USE	*EXECUTE
	Описание устройства ASP	*USE	
WRKSBS ^{2,3}	Описание подсистемы	Любые права доступа	*USE
WRKSBSD ³	Описание подсистемы	Любые права доступа	*USE
¹	Для использования этой команды необходимо иметь специальные права доступа (*JOBCTL).		
²	Необходимы права доступа (любые, за исключением *EXCLUDE)		
³	Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.		
⁴	Для проверки формата файла меню необходимы соответствующие права доступа. Проверка позволяет гарантировать правильность работы меню при запуске подсистемы. Если у пользователя нет прав доступа к файлу меню или его библиотеке, то формат не будет проверен.		
⁵	Для того чтобы указать в качестве библиотеки подсистемы конкретную библиотеку, необходимы специальные права доступа *SECADM или *ALLOBJ.		
⁶	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ или *AUDIT.		
⁷	Для изменения имени группы ASP необходимы специальные права доступа *ALLOBJ и *SECADM.		
⁸	Для указания несуществующего описания ASP необходимы специальные права доступа ко всем объектам (*ALLOBJ).		
⁹	Для указания несуществующего описания задания необходимы специальные права доступа ко всем объектам (*ALLOBJ).		

Системные команды

В этой таблице перечислены права доступа, необходимые для выполнения системных команд.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В разделе Команды, поставляемые с общими правами доступа *EXCLUDE, приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
PWRDWN SYS ¹	Каталог образов (если задан)	*USE	
RTV SYSINF (Q) ²	Библиотека	*READ, *ADD, *EXECUTE	
Для выполнения следующих команд не требуются никакие права доступа к объектам:			
CHGSHRPOOL DSPSYSSTS ENDSYS ¹ PRTSYSINF (Q)	RCLACTGRP ¹ RCLRSC RETURN RTVGRPA	SIGNOFF UPDSYSINF (Q) ³ WRKSHRPOOL	WRKSYSSTS
¹	Для использования этой команды необходимо иметь специальные права доступа (*JOBCTL).		
²	Для выполнения этой команды необходимы специальные права доступа *SAVSYS.		
³	Для выполнения этой команды необходимы специальные права доступа *SECADM, *ALLOBJ, *AUDIT, *JOBCTL и *SAVSYS.		

Команды системного списка ответов

В этой таблице перечислены права доступа, необходимые для выполнения команд системного списка ответов.

Для выполнения этих команд не требуются никакие права доступа к объектам:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

Команды для работы с системными значениями

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с системными значениями.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Для выполнения следующих команд не требуются никакие права доступа к объектам:			
CHGSYSVAL (Q) ^{1,2}	DSPSYSVAL ³	RTVSYSVAL ³	WRKSYSVAL ^{1,2,3}
¹	Для изменения некоторых системных значений необходимы специальные права доступа *ALLOBJ, *ALLOBJ и *SECADM, *AUDIT, *IOSYSCFG или *JOBCTL.		
²	Для применения этой команды в том виде, в котором она поставляется фирмой IBM, необходимо работать в системе под именем QPGMR, QSYSOPR или QSRV или иметь специальные права доступа *ALLOBJ.		
³	Для просмотра или извлечения системных значений, связанных с контролем, необходимы специальные права доступа *AUDIT или *ALLOBJ.		

Команды среды System/36

В этой таблице перечислены права доступа, необходимые для выполнения команд среды System/36.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGS36	Объект конфигурации S/36 QS36ENV	*UPD	*EXECUTE
CHGS36A	Объект конфигурации S/36 QS36ENV	*UPD	*EXECUTE
CHGS36PGMA	Программа	*OBJMGT, *USE	*EXECUTE
CHGS36PRCA	Файл QS36PRC	*OBJMGT, *USE	*EXECUTE
CHGS36SRCA	Исходный файл	*OBJMGT, *USE	*EXECUTE
CRTMSGFMNU	Меню: REPLACE(*NO)		*READ, *ADD
	Меню: REPLACE(*YES)	См. общие правила.	*READ, *ADD
	Файл меню, если он существует	*ALL	*EXECUTE
	Файл сообщений	*USE	*CHANGE
	Исходный файл QS36SRC	*ALL	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTS36DSPF	Файл дисплея: REPLACE(*NO)		*READ, *ADD
	Файл дисплея: REPLACE(*YES)	См. общие правила.	*READ, *ADD, *CHANGE
	Исходный файл приемника, если TOMBR не равно *NONE	*ALL	*CHANGE
	Исходный файл QS36SRC	*USE	*EXECUTE
	Команда Создать файл дисплея (CRTDSPF)	*OBJOPR	*EXECUTE
CRTS36MNU	Меню: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Меню: REPLACE(*YES)	См. общие правила.	*READ, *ADD, *CHANGE
	Исходный файл приемника, если TOMBR не равно *NONE	*ALL	*CHANGE
	Исходный файл QS36SRC	*USE	*EXECUTE
	Файл меню, если задано значение REPLACE(*YES)	*ALL	*EXECUTE
	Файлы сообщений, указанные в исходном тексте	*ALL	*EXECUTE
	Файл дисплея		*CHANGE
	Команда CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Команда ADDMSGD	*OBJOPR	*EXECUTE
	Команда CRTDSPF	*OBJOPR	*EXECUTE
CRTS36MSGF	Файл сообщений: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Файл сообщений: REPLACE(*YES)	См. общие правила.	*READ, *ADD, *CHANGE
	Исходный файл приемника, если TOMBR не равно *NONE	*ALL	*CHANGE
	Исходный файл QS36SRC	*USE	*EXECUTE
	Файл меню, если задано значение REPLACE(*YES)	*ALL	*EXECUTE
	Файл сообщений, указанный в исходном тексте	*ALL	*EXECUTE
	Указанный в исходном тексте файл сообщений, если параметру OPTION присвоено значение *ADD или *CHANGE	*CHANGE	*EXECUTE
	Файлы сообщений, указанные в исходном тексте, если задано OPTION(*CREATE)	*ALL	*EXECUTE
	Команда CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Команда ADDMSGD	*OBJOPR	*EXECUTE
	Команда CHGMSGD, если указано OPTION(*CHANGE)	*OBJOPR	*EXECUTE
DSPS36	Объект конфигурации S/36 QS36ENV	*READ	*EXECUTE
EDTS36PGMA	Программа (при изменении атрибутов)	*OBJMGT, *USE	*EXECUTE
	Программа (при просмотре атрибутов)	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
EDTS36PRCA	Файл QS36PRC (при изменении атрибутов)	*OBJMGT, *USE	*EXECUTE
	Файл QS36PRC (при просмотре атрибутов)	*USE	*EXECUTE
EDTS36SRCA	Исходный файл QS36SRC (при изменении атрибутов)	*OBJMGT, *USE	*EXECUTE
	Исходный файл QS36SRC (при просмотре атрибутов)	*USE	*EXECUTE
RSTS36F (Q)	Исходный файл	*USE	*EXECUTE
	Целевой файл	*ALL	См. общие правила.
	Базовый физический файл, если восстанавливаемый файл - это логический (альтернативный) файл	*CHANGE	*EXECUTE
	Файл устройства или описание устройства	*USE	*EXECUTE
RSTS36FLR ^{1,2,3} (Q)	Папка S/36	*USE	*EXECUTE
	Целевая папка	*CHANGE	*EXECUTE
	Файл устройства или описание устройства	*USE	*EXECUTE
RSTS36LIBM (Q)	Исходный файл	*USE	*EXECUTE
	Целевой файл	*ALL	См. общие правила.
	Файл устройства или описание устройства	*USE	*EXECUTE
RTVS36A	Объект конфигурации S/36 QS36ENV	*UPD	*EXECUTE
SAVS36F	Исходный файл	*USE	*EXECUTE
	Целевой файл, если это физический файл	*ALL	См. общие правила.
	Файл устройства или описание устройства	*USE	*EXECUTE
SAVS36LIBM	Исходный файл	*USE	*EXECUTE
	Целевой файл, если это физический файл	*ALL	См. общие правила.
	Файл устройства или описание устройства	*USE	*EXECUTE
WRKS36	Объект конфигурации S/36 QS36ENV	*READ	*EXECUTE
WRKS36PGMA	Программа (при изменении атрибутов)	*OBJMGT, *USE	*EXECUTE
	Программа (при просмотре атрибутов)	*USE	*EXECUTE
WRKS36PRCA	Файл QS36PRC (при изменении атрибутов)	*OBJMGT, *USE	*EXECUTE
	Файл QS36PRC (при просмотре атрибутов)	*USE	*EXECUTE
WRKS36SRCA	Исходный файл QS36SRC (при изменении атрибутов)	*OBJMGT, *USE	*EXECUTE
	Исходный файл QS36SRC (при просмотре атрибутов)	*USE	*EXECUTE
¹	Для замены документа необходимы все (*ALL) права доступа к этому документу. Для восстановления новой информации в папке необходимы операционные права доступа к папке и все права доступа к данным папки, либо специальные права доступа *ALLOBJ.		
²	Если применяется к словарю данных, то достаточно прав на выполнение команды.		
³	Если исходная папка является папкой документов, то пользователь должен быть зарегистрирован в системном каталоге рассылки.		

Команды для работы с таблицами

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с таблицами.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTTBL	Таблица		*READ, *ADD, *EXECUTE
	Исходный файл	*USE	*EXECUTE
DLTTBL	Таблица	*OBJEXIST	*EXECUTE
WRKTBL ¹	Таблица	Любые права доступа	*USE
¹ Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.			

Команды TCP/IP

В этой таблице перечислены права доступа, необходимые для команд работы с TCP/IP.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ADDTCPSVR ¹	Вызываемая программа	*EXECUTE	*EXECUTE
CHGTCPVSR ¹	Вызываемая программа	*EXECUTE	*EXECUTE
SPYTCRPT ⁶	Объекты файлов		
CVTTCPCPL (Q)	Объекты файлов	*USE	*EXECUTE
ENDTCPPTP	Описание линии ⁴	*USE	*EXECUTE
	Описание контроллера ⁴	*USE	*EXECUTE
	Описание устройства ⁴	*USE	*EXECUTE
	Объекты файлов	*USE	*EXECUTE
ENDTCPSRV (Q)	Объекты файлов	*USE	*EXECUTE
FTP	Объекты файлов	*USE	*EXECUTE
	Объекты таблиц	*USE	*EXECUTE
LPR ²	Объект настройки рабочей станции	*USE	*EXECUTE
SETVTTBL	Объекты таблиц	*USE	*EXECUTE
SNDTCPSPLF ²	Объект настройки рабочей станции	*USE	*EXECUTE
STRTCPFPT	Объекты таблиц	*USE	*EXECUTE
	Объекты файлов	*USE	*EXECUTE
STRTCPPTP	Описание линии ⁴	*USE	*EXECUTE
	Описание контроллера ⁴	*USE	*EXECUTE
	Описание устройства ⁴	*USE	*EXECUTE
	Объекты файлов	*USE	*EXECUTE

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
STRTCPSVR (Q)	Объекты таблиц	*USE	*EXECUTE
	Объекты файлов	*USE	*EXECUTE
STRTCPTELN	Объекты таблиц	*USE	*EXECUTE
	Объекты файлов	*USE	*EXECUTE
	Виртуальная рабочая станция ⁵	*USE	*EXECUTE
TELNET	Объекты таблиц	*USE	*EXECUTE
	Объекты файлов	*USE	*EXECUTE
	Виртуальная рабочая станция ⁵	*USE	*EXECUTE
Для выполнения следующих команд не требуются никакие права доступа к объектам:			
ADDCOMSNMP ¹	CFGRTG	CHGVTMAP	RMVTCPRSI ¹
ADDNETBLE ¹	CFGTCPSMTP	DSPVTMAP	RMVTCPRTE ¹
ADDOSPFARA ¹	CFGTCPSNMP	ENDTCP (Q)	RMVTCPSVR ¹
ADDOSPFLNK ¹	CFGTCPTELN	ENDTCPCNN	RNMTCPHTE ¹
ADDOSPFIFC ¹	CHGCOMSNMP ¹	ENDTCPIFC (Q)	SETVTMAP
ADDOSPFNRNG ¹	CHGFTPA ¹	MGRTCPHT ¹	STRTCP (Q)
ADDPCLTBLE ¹	CHGLPDA ¹	NETSTAT	STRTCPIFC (Q)
ADDRIPACP ¹	CHGOSPFA ¹	PING	VFYTCPCNN
ADDRIPFLT ¹	CHGOSPFA ¹	RMVCOMSNMP ¹	WRKNAMSMTP ³
ADDRIPFC ¹	CHGOSPFI ¹	RMVNETTBLE ¹	WRKNETTBLE ¹
ADDRIPIGN ¹	CHGOSPFLNK ¹	RMVOSPFARA ¹	WRKPCLTBLE ¹
ADDSRVTBLE ¹	CHGOSPFNRNG ¹	RMVOSPFIFC ¹	WRKSRVTBLE ¹
ADDTCPHTE ¹	CHGRIPA ¹	RMVOSPFLNK ¹	WRKTCPSTS
ADDTCPIFC ¹	CHGRIPFLT ¹	RMVOSPFNRNG ¹	
ADDTCPPORT ¹	CHGRIPIFC ¹	RMVPCLTBLE ¹	
ADDTCPRSI ¹	CHGSMTPA ¹	RMVRIPACP ¹	
ADDTCPRTE ¹	CHGSMMPA ¹	RMVRIPFLT ¹	
CFGTCP	CHGTCPA ¹	RMVRIPIFC ¹	
CFGTCPAPP	CHGTCPHTE ¹	RMVRIPIGN ¹	
CFGTCPFTP ¹	CHGTCPIFC ¹	RMVSRVTBLE ¹	
CFGTCPLPD ¹	CHGTCPRTE ¹	RMVTCPHTE ¹	
	CHGTELNA ¹	RMVTCPIFC ¹	
		RMVTCPPORT ¹	
¹	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.		
²	Для применения команд SNDTCPSPLF и LPR требуется та же комбинация прав доступа, что и для команды SNDNETSPLF.		
³	Для изменения таблицы псевдонимов системы или профайла другого пользователя необходимы специальные права доступа *SECADM.		
⁴	Если у вас есть специальные права доступа *JOBCTL, то указанные права доступа не нужны.		
⁵	Если у вас есть специальные права доступа *JOBCTL, то указанные права доступа к объекту в удаленной системе не нужны.		
⁶	Необходимые права доступа описаны в разделе Общие правила для прав доступа команд к объектам для операции Показать (DSP) или другой операции, использующей файл вывода (OUTPUT (*OUTFILE))		

Команды описания часового пояса

В этой таблице перечислены права доступа, необходимые для выполнения команд описания часового пояса.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CHGTIMZON	Описание часового пояса	*CHANGE	*EXECUTE
CRTTIMZON	Описание часового пояса		*READ, *ADD
DLTTIMZON ¹	Описание часового пояса	*OBJEXIST	*EXECUTE
WRKTIMZON ²	Описание часового пояса	*USE	*USE
¹ Удалить описание часового пояса, указанное в системном значении QTIMZON, нельзя. ² Если в сообщении указаны сокращенное и полное имена часового пояса, то для просмотра этих имен необходимо обладать правами на использование (*USE) файла сообщений и правами доступа *EXECUTE к библиотеке файла сообщений.			

Команды для работы с информацией о заказе на обновление

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с информацией о заказе на обновление.

Эти команды поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
WRKORDINF	Файл QGPL/QMANFILE	*CHANGE, *OBJALTER	*EXECUTE

Команды для работы с пользовательским индексом, пользовательской очередью и пользовательским пространством

В этой таблице перечислены права доступа, необходимые для выполнения команд с пользовательским индексом, пользовательской очередью и пользовательским пространством.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
DLTUSRIDX	Пользовательский индекс	*OBJEXIST	*EXECUTE
DLTUSRQ	Пользовательская очередь	*OBJEXIST	*EXECUTE
DLTUSRSPC	Пользовательское пространство	*OBJEXIST	*EXECUTE

Команды для работы с пользовательской файловой системой

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с пользовательской файловой системой.

Команда	Объект	Тип объекта	Файловая система	Требуемые права доступа к объекту
ADDMFS ^{1,2,3}	Каталог, в котором выполняется монтирование	*DIR	корневая (/)	*W
	Префикс пути	См. общие правила.		
CRTUDFS ^{1,2,6,7} (Q)	/dev/QASPxx или /dev/IASPname	*DIR	корневая (/)	*RWX
DLTUDFS ^{1,2,4,5,8,9,10} (Q)	/dev/QASPxx или /dev/IASPname	*DIR	корневая (/)	*RWX
	любой объект интегрированной файловой системы в UDFS		корневая (/)	*OBJEXIST
	Любой непустой объект каталога	*DIR	корневая (/)	*WX
DSPUDFS	Каталог	*DIR	корневая (/)	*RX
MOUNT ^{1,2,3}	каталог-монтирования	*DIR	корневая (/)	*W
	Префикс пути	См. общие правила.		
RMVMFS ¹				
UNMOUNT ¹				
¹	Для выполнения этой команды необходимы специальные права доступа *IOSYSCFG.			
²	Существует два возможных соглашения об именах каталогов, в зависимости от местонахождения пользовательской файловой системы (UDFS). Выберите одно из следующих соглашений: <ul style="list-style-type: none"> • - /dev/QASPxx, где xx - это 01 для системного ASP и 02-32 для базовых пользовательских ASP. • - /dev/имя_IASP, где <i>имя_IASP</i> - это имя независимого ASP. Это каталог, содержащий монтируемый объект *BLKSF.			
³	Каталог, в котором выполняется монтирование - это любой каталог интегрированной файловой системы, в котором необходимо смонтировать файловую систему.			
⁴	UDFS может содержать целое поддерево объектов, поэтому удаляя UDFS, вы удаляете объекты всех типов, которые могут храниться в пользовательской файловой системе.			
⁵	Для применения команд DLTUDFS необходимы права к существованию (*OBJEXIST) всех объектов UDFS, в противном случае никакие объекты удалены не будут.			
⁶	Для применения этой команды со значением параметра Опция поиска объектов (CRTOBJSCAN), отличным от *PARENT, необходимы специальные права доступа ко всем объектам (*ALLOBJ) и права администратора защиты (*SECADM).			
⁷	Если в параметре Значение контроля объектов (CRTOBJAUD) указано значение, отличное от *SYSVAL, то для выполнения этой команды необходимы специальные права на контроль (*AUDIT).			
⁸	У вас должны быть права на запись (*W) и на выполнение (*X) ко всем непустым объектам каталогов в UDFS.			
⁹	Если у какого-либо непустого объекта каталога в UDFS атрибут "Переименование и удаление ссылки запрещено" равен Да (этот атрибут эквивалентен биту режима S_ISVTX), то должно быть выполнено по крайней мере одно из следующих условий: <ul style="list-style-type: none"> • Вы должны быть владельцем всех объектов этого каталога. • Вы должны быть владельцем этого каталога. • У вас должны быть специальные права доступа ко всем объектам (*ALLOBJ). 			
¹⁰	UDFS невозможно удалить, если она содержит объект, атрибут <i>read only</i> которого равен <i>yes</i> , или если она содержит исключенный из списка объект.			

Команды для работы с пользовательским профайлом

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с пользовательским профайлом.

Команды, помеченные буквой (Q), поставляются с общими правами доступа *EXCLUDE. В Приложение С, “Команды, поставляемые с общими правами доступа *EXCLUDE”, на стр. 347 приведен список поставляемых IBM пользовательских профайлов, у которых есть права доступа к этим командам. Системный администратор может предоставлять права доступа *USE другим пользователям.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
ANZDFTPWD ^{3, 14, 15(Q)}			
ANZPRFACT ^{3, 14, 15(Q)}			
CHGACTPRFL ^{14(Q)}			
CHGACTSCDE ^{3, 14, 15(Q)}			
CHGDSTPWD ¹			
CHGEXPSCDE ^{3, 14, 15(Q)}			
CHGPRF	Пользовательский профайл	*OBJMGT, *USE	
	Начальная программа ²	*USE	*EXECUTE
	Начальное меню ²	*USE	*EXECUTE
	Описание задания ²	*USE	*EXECUTE
	Очередь сообщений ²	*USE	*EXECUTE
	Очередь вывода ²	*USE	*EXECUTE
	Программа реакции на клавишу Attention ²	*USE	*EXECUTE
	Текущая библиотека ²	*USE	*EXECUTE
CHGPWD			
CHGUSRAUD ^{11(Q)}			
CHGUSRPRF ³	Пользовательский профайл	*OBJMGT, *USE	*EXECUTE
	Начальная программа ²	*USE	*EXECUTE
	Начальное меню ²	*USE	*EXECUTE
	Описание задания ²	*USE	*EXECUTE
	Очередь сообщений ²	*USE	*EXECUTE
	Очередь вывода ²	*USE	*EXECUTE
	Программа реакции на клавишу Attention ²	*USE	*EXECUTE
	Текущая библиотека ²	*USE	*EXECUTE
	Групповой профайл (GRPPRF или SUPGRPPRF) ^{2,4}	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CHGUSRPRTI	Пользовательский профайл	*CHANGE	
CHKPWD			

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTUSRPRF ^{3, 12, 17}	Начальная программа	*USE	*EXECUTE
	Начальное меню	*USE	*EXECUTE
	Описание задания	*USE	*EXECUTE
	Очередь сообщений	*USE	*EXECUTE
	Очереди вывода	*USE	*EXECUTE
	Программа реакции на клавишу Attention	*USE	*EXECUTE
	Текущая библиотека	*USE	*EXECUTE
	Групповой профайл (GRPPRF или SUPGRPPRF) ⁴	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CVTUSRCERT ^{3, 14}			
DLTUSRPRF ^{3, 9}	Пользовательский профайл	*OBJEXIST, *USE	*EXECUTE
	Очередь сообщений ⁵	*OBJEXIST, *USE, *DLT	*EXECUTE
DMPUSRPRF ^{22(Q)}	Пользовательский профайл		
DSPACTPRFL ^{14(Q)}			
DSPACTSCD ^{14(Q)}			
DSPAUTUSR ⁶	Пользовательский профайл	*READ	
DSPEXPSCD ^{14(Q)}			
DSPPGMADP	Пользовательский профайл	*OBJMGT	
	Файл вывода	См. общие правила.	См. общие правила.
DSPSSTUSR ²³			
DSPUSRPRF ¹⁹	Пользовательский профайл	*READ	*EXECUTE
	Файл вывода	См. общие правила.	См. общие правила.
DSPUSRPTI	Пользовательский профайл	*USE	
GRTUSRAUT ⁷	Пользовательский профайл, к которому выполняется обращение	*READ	
	Объекты, к которым предоставляются права доступа	*OBJMGT	*EXECUTE
PRTPRFINT ^{14(Q)}			
PRTUSRPRF ¹⁸			
RSTAUT (Q) ⁸			
RSTUSRPRF (Q) ^{8, 10, 16}			
RTVUSRPRF ²⁰	Пользовательский профайл	*READ	
RTVUSRPTI	Пользовательский профайл	*USE	
SAVSECDTA ⁸	Файл сохранения, если он пуст	*USE, *ADD	*EXECUTE
	Файл сохранения (если в нем есть записи)	*OBJMGT, *USE, *ADD	*EXECUTE
WRKUSRPRF ¹³	Пользовательский профайл	Любые права доступа	

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
1	Выполнить эту команду может только пользователь, работающий в системе под именем QSECOFR.		
2	Необходимы права доступа только к тем объектам, которые соответствуют изменяемым полям пользовательского профайла.		
3	Необходимы специальные права доступа *SECADM.		
4	Права доступа *OBJMGT к групповому профайлу не могут следовать из принятых прав доступа.		
5	Очередь сообщений, связанная с пользовательским профайлом, удаляется, если она принадлежит этому профайлу. Для удаления очереди сообщений у пользователя, выполняющего команду DLTUSRPRF, должны быть указанные права доступа.		
6	Будут показаны только те пользовательские профайлы, права доступа к которым есть у пользователя, выполняющего команду.		
7	См. права доступа, необходимые для команды GRTOBJAUT.		
8	Необходимы специальные права доступа *SAVSYS.		
9	Если вы применяете эту команду для удаления объектов, принадлежащих пользовательскому профайлу, то необходимы также права на удаление. Если вы применяете команду для передачи объектов другому профайлу, то вам потребуются соответствующие права доступа к объектам и к целевому профайлу. См. информацию о команде CHGOBJOWN.		
10	Для того чтобы присвоить параметру Разрешить различия в объектах (ALWOBJDIF) значение, отличное от *NONE, необходимы специальные права доступа *ALLOBJ.		
11	Необходимы специальные права доступа *AUDIT.		
12	Пользователь, для которого создается профайл, будет обладать следующими правами доступа к нему: *OBJMGT, *OBJOPR, *READ, *ADD, *DLT, *UPD, *EXECUTE.		
13	Для выполнения отдельной операции необходимы права доступа, соответствующие этой операции.		
14	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ.		
15	Для выполнения этой команды необходимы специальные права доступа *JOBCTL.		
16	Для применения этой команды с параметрами SECDDA(*PWDGRP), USRPRF(*ALL) или OMITUSRPRF необходимы права доступа *ALLOBJ и *SECADM.		
17	С помощью команды CRTUSRPRF нельзя создать пользовательский профайл (*USRPRF) в независимом пуле дисков. Однако, если пользователь обладает частными правами доступа к объекту из независимого пула дисков, является владельцем такого объекта или входит в состав основной группы этого объекта в независимом пуле дисков, то имя пользовательского профайла хранится в независимом пуле дисков. В случае перемещения независимого пула дисков в другую систему записи о частных правах доступа, принадлежности объектов и основных группах прикрепляются к пользовательскому профайлу с тем же именем в целевой системе. Если в целевой системе нет такого профайла, то он будет создан. При этом пользователю не предоставляются специальные права доступа, а в качестве пароля указывается значение *NONE.		
18	Для выполнения этой команды необходимы специальные права доступа *ALLOBJ или *AUDIT.		
19	Для просмотра текущих значений контроля объекта и контроля действия необходимы специальные права доступа *ALLOBJ или *AUDIT. В противном случае будет возвращено значение *NOTAVL, указывающее, что эти значения недоступны для просмотра.		
20	Для извлечения текущих значений OBJAUD и AUDLVL необходимы специальные права доступа *ALLOBJ или *AUDIT. В противном случае будет возвращено значение *NOTAVL, указывающее, что эти значения недоступны для извлечения.		

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
21	Для применения этой команды у вас должны быть специальные права на обслуживание (*SERVICE) или права доступа к функции Служебный дамп i5/OS посредством функции Администрирование приложений System i Navigator. Изменить список пользователей, которые могут создавать служебный дамп, можно и с помощью команды Изменить права доступа к функции (CHGFCNUSG) с ИД функции QIBM_SERVICE_DUMP.		
22	Для применения этой команды у вас должны быть специальные права доступа *SERVICE или права доступа к функции QIBM_SERVICE_DUMP.		
23	Для выполнения этой команды необходимы права доступа администратора защиты (*SECADM) или специальные права на контроль (*AUDIT).		

Команды для работы с контрольным списком

В этой таблице перечислены права доступа, необходимые для выполнения команд контрольного списка.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTVLDL	Контрольный список		*ADD, *READ
DLTVLDL	Контрольный список	*OBJEXIST	*EXECUTE

Команды настройки рабочей станции

В этой таблице перечислены права доступа, необходимые для выполнения команд настройки рабочей станции.

Команда	Объект	Необходимые права доступа	
		К объекту	К библиотеке
CRTWSCST	Исходный файл	*USE	*EXECUTE
	Объект настройки рабочей станции, если REPLACE(*NO)		*READ, *ADD
	Объект настройки рабочей станции, если REPLACE(*YES)	*OBJMGT, *OBJEXIST	*READ, *ADD
DLTWSCST	Объект настройки рабочей станции	*OBJEXIST	*EXECUTE
RTVWSCST	Целевой файл, если он существует и в него добавляется новый элемент	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Целевой файл, если файл и элемент существуют	*OBJOPR, *ADD, *DLT	*EXECUTE
	Целевой файл, если файл не существует		*READ, *ADD

Команды для работы с загрузчиками

В этой таблице перечислены права доступа, необходимые для выполнения команд для работы с загрузчиками.

Команда	Объект	Параметры очереди вывода		Специальные права доступа	Необходимые права доступа	
		AUTCHK	OPRCTL		К объекту	К библиотеке
CHGWTR ^{2,4}	Текущая очередь вывода ¹	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Владелец ³	
			*YES	*JOBCTL		
	Новая очередь вывода	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Владелец	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
ENDWTR ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Владелец ³	
			*YES	*JOBCTL		
HLDWTR ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Владелец ³	
			*YES	*JOBCTL		
RLSWTR ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Владелец ³	
			*YES	*JOBCTL		
STRDKTWTR ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Владелец ³	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Очередь сообщений				*OBJOPR, *ADD	*EXECUTE
	Описание устройства				*OBJOPR, *READ	

Команда	Объект	Параметры очереди вывода		Специальные права доступа	Необходимые права доступа	
		AUTCHK	OPRCTL		К объекту	К библиотеке
STRPRTWTR ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Владелец ³	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Очередь сообщений				*OBJOPR, *ADD	*EXECUTE
	Объект настройки рабочей станции				*USE	*EXECUTE
	Программа польз. драйвера				*OBJOPR *EXECUTE	*EXECUTE
	Программа преобразования польз. данных				*OBJOPR *EXECUTE	*EXECUTE
	Польз. программа разделителя				*OBJOPR *EXECUTE	*EXECUTE
	Описание устройства				*OBJOPR, *READ	
STRRMWTR ¹	Очереди вывода	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Владелец ³	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Очередь сообщений				*OBJOPR, *ADD	*EXECUTE
	Объект настройки рабочей станции				*USE	*EXECUTE
	Программа польз. драйвера				*OBJOPR *EXECUTE	*EXECUTE
	Программа преобразования польз. данных				*OBJOPR *EXECUTE	*EXECUTE
WRKWTR						
¹	Если у вас есть специальные права доступа *SPLCTL, то указанные права доступа к очереди вывода не нужны.					
²	Для изменения очереди вывода загрузчика необходимо наличие одного из указанных здесь типов прав доступа к новой очереди вывода.					
³	Необходимо являться владельцем очереди вывода.					
⁴	Права доступа *EXECUTE к библиотеке новой очереди вывода необходимы даже в том случае, когда у пользователя есть специальные права доступа *SPLCTL.					

Приложение Е. Работа с объектами и контроль за объектами

В этом разделе перечислены операции, которые можно выполнять над объектами системы, и приведена информация о том, какие из этих операций контролируются.

Список структурирован по типам объектов. В отдельные группы объединены операции, которые контролируются в том случае, если в параметре OBJAUD команды CHGOBJAUD или CHGDLOAUD было задано значение *ALL или *CHANGE.

Контрольная запись о выполнении действия заносится только при определенном сочетании системных значений, включая значение из профайла пользователя, выполняющего операцию, и значение, заданное для объекта. В “Планирование контроля доступа к объектам” на стр. 304 приведена информация о настройке контроля за объектами.

Названия операций указаны в таблице прописными буквами (например, CPYF) и обозначают имена соответствующих команд CL, если явно не указано, что они представляют интерфейсы прикладных программ (API).

Общие операции для всех типов объектов

В этом списке указаны общие операции для всех типов объектов и условия их контроля.

- Операция чтения

CRTDUPOBJ

Создать копию объекта (если в параметре "*исходный-объект*" указано значение *ALL).

DMPOBJ

Создать дамп объекта

DMPSYSOBJ

Создать дамп системного объекта

QSRSAVO

API Сохранить объект

QsrSave

API Сохранить объект в каталоге

SAV

Сохранить объект в каталоге

SAVCHGOBJ

Сохранить измененный объект

SAVLIB

Сохранить библиотеку

SAVOBJ

Сохранить объекты

SAVSAVFDTA

Сохранить данные файла сохранения

SAVDLO

Сохранить объект DLO

SAVLICPGM

Сохранить лицензионную программу

SAVSHF

Сохранить книжную полку

Примечание: В контрольной записи операции сохранения будет указано, выполнялось ли сохранение с параметром STG(*FREE).

- Операция изменения

APYJRNCHG

Применить зарегистрированные изменения

CHGJRNOBJ

Изменить объект с журналом

CHGOBJD

Изменить описание объекта

CHGOBJOWN

Изменить владельца объекта

CRTxxxxxx

Создать объект

Notes:

1. Если в качестве целевой библиотеки указано значение *ALL или *CHANGE, то при создании объекта в журнал заносится запись ZC.
2. Если для контроля действий задано значение *CREATE, то при создании объекта в журнал заносится запись CO.

DLTxxxxxx

Удалить объект

Notes:

1. Если в качестве библиотеки объекта задано значение *ALL или *CHANGE, то при удалении объекта в журнал заносится запись ZC.
2. Если в качестве объекта задано значение *ALL или *CHANGE, то при его удалении в журнал заносится запись ZC.
3. Если для контроля действий задано значение *DELETE, то при удалении объекта в журнал заносится запись DO.

ENDJRNxxx

Завершить ведение журнала

GRTOBJAUT

Предоставить права доступа к объекту

Примечание: Если для предоставления прав доступа используется модельный объект, то контрольная запись для указанного модельного объекта не создается.

MOV OBJ

Переместить объект

QjoEndJournal

Завершить ведение журнала

QjoStartJournal

Начать ведение журнала

QSRRSTO

API Восстановить объект

QsrRestore

API Восстановить объект в каталоге

RCLSTG

Восстановить память:

- Если *AUTL объекта поврежден, и для его защиты устанавливается список прав доступа QRCLAUTL, то создается контрольная запись.
- При перемещении объекта в библиотеку QRCL создается контрольная запись.

RMVJRNCHG

Удалить зарегистрированные изменения

RNMOBJ

Переименовать объект

RST Восстановить объект в каталоге

RSTCFG

Восстановить объекты конфигурации

RSTLIB

Восстановить библиотеку

RSTLICPGM

Восстановить лицензионную программу

RSTOBJ

Восстановить объект

RVKOBJAUT

Аннулировать права доступа к объекту

STRJRNxxx

Начать ведение журнала

- Операции, для которых не включен контроль

Приглашение¹

Программа переопределения приглашения для команды изменения (если она существует)

CHKOBJ

Проверить объект

ALCOBJ

Захватить объект

CPOBJ

Сжать объект

DCPOBJ

Развернуть объект

DLCOBJ

Освободить объект

DSPOBJD

Показать описание объекта

DSPOBJAUT

Показать права доступа к объекту

1. Программа переопределения приглашения показывает текущие значения при просмотре приглашения команды. Например, если вы введете CHGURSPRF USERA и нажмете F4 (приглашение), то появится меню Изменить пользовательский профайл, в котором будут указаны текущие значения параметров пользовательского профайла USERA.

EDTOBJAUT

Редактировать права доступа к объекту

Примечание: Если в функции контроля действий задано значение *SECURITY, либо включен контроль за объектом, то при изменении прав доступа к объекту создается контрольная запись.

QSYCUSRA

API Проверить права доступа к объекту, предоставленные пользователю

QSYLUSRA

API Показать пользователей с правами доступа к объекту. Для объекта, информацию о котором показывает API, контрольная запись не создается. Однако контрольная запись создается для пользовательского пространства, содержащего информацию.

QSYRUSRA

API Получить права доступа к объекту, предоставленные пользователю

RCLTMPSTG

Восстановить временную память

RMVDFRID

Удалить отложенный ИД

RSTDFROBJ

Восстановить отложенный объект

RTVOBJD

Получить описание объекта

SAVSTG

Сохранить содержимое памяти (контроль только за командой SAVSTG)

WRKOBJLCK

Работа с блокировкой объекта

WRKOBJOWN

Работа с объектами по владельцу

WRKxxx

Команды работы с объектами

Операции над временем восстановления путей доступа

В этом списке указаны операции, выполняемые над объектом времени восстановления путей доступа, и условия их контроля.

Примечание: Изменение времени восстановления путей доступа контролируется в том случае, если в системном значении Контроль действий (QAUDLVL) или параметре пользовательского профайла Контроль действий (AUDLVL) задано значение *SYSMGT.

- Операции, для которых включен контроль

CHGRCYAP

Изменить восстановление путей доступа

EDTRCYAP

Редактировать восстановление путей доступа

- Операции, для которых контроль не включен

DSPRCYAP

Показать параметры восстановления путей доступа

Операции над таблицей предупреждений (*ALRTBL)

В этом списке указаны операции, выполняемые над таблицей предупреждений (*ALRTBL), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

ADDALRD

Добавить описание предупреждения

CHGALRD

Изменить описание предупреждения

CHGALRTBL

Изменить таблицу предупреждений

RMVALRD

Удалить описание предупреждения

- Операции, для которых контроль не включен

Печать

Печать описания предупреждения

WRKALRD

Работа с описанием предупреждения

WRKALRTBL

Работа с таблицей предупреждений

Операции над списком прав доступа (*AUTL)

В этом списке указаны операции, выполняемые над списком прав доступа (*AUTL), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

ADDAUTLE

Добавить запись списка прав доступа

CHGAUTLE

Изменить запись списка прав доступа

EDTAUTL

Редактировать список прав доступа

RMVAUTLE

Удалить запись списка прав доступа

- Операции, для которых контроль не включен

DSPAUTL

Показать список прав доступа

DSPAUTLOBJ

Показать объекты списка прав доступа

DSPAUTLDLO

Показать DLO списка прав доступа

RTVAUTLE

Получить запись списка прав доступа

QSYLATLO

API Показать объекты, защищенные с помощью *AUTL

WRKAUTL

Работа со списком прав доступа

Операции над владельцем прав доступа (*AUTHLR)

В этом списке указаны операции, выполняемые над владельцем прав доступа (*AUTHLR), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

Сопутствующие

Когда применяется для защиты объекта.

- Операции, для которых контроль не включен

DSPAUTHLR

Показать владельца прав доступа

Операции над каталогом связывания (*BNDDIR)

В этом списке указаны операции, выполняемые над каталогом связывания (*BNDDIR), и условия их контроля.

- Операция чтения

CRTPGM

Создать программу

CRTSRVPGM

Создать служебную программу

RTVBNSRC

Получить исходный файл редактора связей

UPDPGM

Обновить программу

UPDSRVPGM

Обновить служебную программу

- Операция изменения

ADDBNDDIRE

Добавить записи каталога связывания

RMVBNDDIRE

Удалить записи каталога связывания

- Операции, для которых контроль не включен

DSPBNDDIR

Показать содержимое каталога связывания

WRKBNDDIR

Работа с каталогом связывания

WRKBNDDIRE

Работа с записью каталога связывания

Операции над списком конфигурации (*CFGL)

В этом списке указаны операции, выполняемые над списком конфигурации (*CFGL), и условия их контроля.

- Операция чтения

CPYCFGL

Скопировать список конфигурации. Запись создается для *исходного списка конфигурации*.

- Операция изменения

ADDCFGL

Добавить записи списка конфигурации

CHGCFGL

Изменить список конфигурации

CHGCFGLE

Изменить запись списка конфигурации

RMVCFGLE

Удалить запись списка конфигурации

- Операции, для которых контроль не включен

DSPCFGL

Показать список конфигурации

WRKCFGL

Работа со списком конфигурации

Операции над специальными файлами (*CHRSF)

В этом списке указаны операции, выполняемые над специальными файлами (*CHRSF), и условия их контроля.

Информация о контроле за объектами *CHRSF приведена в разделе Операции над потоковым файлом (*STMF).

Операции над форматом диаграммы (*CHTFMT)

В этом списке указаны операции, выполняемые над форматом диаграммы (*CHTFMT), и условия их контроля.

- Операция чтения

Просмотр

Команда DSPCHT или опция F10 в меню BGU

Вывести на принтер/графопостроитель

Команда DSPCHT или опция F15 в меню BGU

Сохранить/создать

Для сохранения и создания файлов графических данных (GDF) применяется команда CRTGDF или опция F13 в меню BGU

- Операция изменения

Нет

- Операции, для которых контроль не включен

Нет

Операции над описанием локали C (*CLD)

В этом списке указаны операции, выполняемые с описанием локали C (*CLD), и условия их контроля.

- Операция чтения

RTVCLDSRC

Получить исходный текст для локали C

Setlocale

Для работы с этим объектом локали C в программах на языке C может применяться функция Set locale.

- Операция изменения

Нет

- Операции, для которых контроль не включен

Нет

Операции с описанием запроса на изменение (*CRQD)

В этом списке указаны операции, выполняемые с описанием запроса на изменение (*CRQD), и условия их контроля.

- Операция чтения

QFVLSTA

API Показать действия над описанием запроса на изменение

QFVRTVCD

API Получить описание запроса на изменение

SBMCRQ

Передать на выполнение запрос на изменение

- Операция изменения

ADDCMDCRQA

Добавить операцию запроса на изменение команды

ADDOBJCRQA

Добавить операцию запроса на изменение объекта

ADDPRDCRQA

Добавить операцию запроса на изменение продукта

ADDPTFCRQA

Добавить операцию запроса на изменение PTF

ADDRSCCRQA

Добавить операцию запроса на изменение ресурса

CHGCMDCRQA

Изменить операцию запроса на изменение команды

CHGCRQD

Изменить описание запроса на изменение

CHGOBJCRQA

Изменить операцию запроса на изменение объекта

CHGPRDCRQA

Изменить операцию запроса на изменение продукта

CHGPTFCRQA

Изменить операцию запроса на изменение PTF

CHGRSCCRQA

Изменить операцию запроса на изменение ресурса

QFVADDA

API Добавить операцию в описание запроса на изменение

QFVRMVA

API Удалить операцию из описания запроса на изменение

RMVCRQDA

Удалить операцию из описания запроса на изменение

- Операции, для которых контроль не включен

WRKCRQD

Работа с описаниями запросов на изменение

Операции над классами (*CLS)

В этом списке указаны операции, выполняемые над классами (*CLS), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

CHGCLS

Изменить класс

- Операции, для которых контроль не включен

Запуск задания

Когда применяется средствами управления заданиями для запуска задания

DSPCLS

Показать класс

WRKCLS

Работа с классом

Операции над командами (*CMD)

В этом списке указаны операции, выполняемые над командами (*CMD), и условия их контроля.

- Операция чтения

Запуск При выполнении команды

- Операция изменения

CHGCMD

Изменить команду

CHGCMDDFT

Изменить значение по умолчанию для команды

- Операции, для которых контроль не включен

DSPCMD

Показать команду

PRTCMDUSG

Печать формата команды

QCRCMDI

API Получить информацию о команде

WRKCMD

Работа с командой

Следующие команды применяются в программах на CL для управления обработкой и для работы с данными в программе. Применение этих команд не контролируется.

CALL ¹ CALLPRC CHGVAR COPYRIGHT DCL DCLF DO ELSE ENDDO	ENDPGM ENDRCV GOTO IF MONMSG PGM	RCVF RETURN SNDF SNDRCVF TFRCTL WAIT
¹ Выполнение команды CALL контролируется в том случае, если она запущена в интерактивном режиме. Выполнение этой команды в программе на CL не контролируется.		

Операции над списком соединений (*CNNL)

В этом списке указаны операции, выполняемые над списком соединений (*CNNL), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

ADDCNNLE

Добавить запись списка соединений

CHGCNNL

Изменить список соединений

CHGCNNLE

Изменить запись списка соединений

RMVCNNLE

Удалить запись списка соединений

RNMCNNLE

Переименовать запись списка соединений

- Операции, для которых контроль не включен

Копирование

Опция 3 меню WRKCNNL

DSPCNNL

Показать список соединений

RTVCFGSRC

Получить исходный текст списка соединений

WRKCNNL

Работа со списком соединений

WRKCNNLE

Работа с записью списка соединений

Операции над описанием класса обслуживания (*COSD)

В этом списке указаны операции, выполняемые над описанием класса обслуживания (*COSD), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

CHGCOSD

Изменить описание класса обслуживания

- Операции, для которых контроль не включен

DSPCOSD

Показать описание класса обслуживания

RTVCFGSRC

Получить исходный текст описания класса обслуживания

WRKOSD

Скопировать описание класса обслуживания

WRKOSD

Работа с описанием класса обслуживания

Операции над исходной информацией связи (*CSI)

В этом списке указаны операции, выполняемые над исходной информацией связи (*CSI), и условия их контроля.

- Операция чтения

DSPCSI

Показать исходную информацию связи

Инициализация

Инициализировать диалог

- Операция изменения

CHGCSI

Изменить исходную информацию связи

- Операции, для которых контроль не включен

WRKCSI

Работа с исходной информацией связи

Операции над списком межсистемных продуктов (*CSPMAP)

В этом списке указаны операции, выполняемые над списком межсистемных продуктов (*CSPMAP), и условия их контроля.

- Операция чтения

Справочник

Когда упоминается в приложении CSP

- Операция изменения

Нет

- Операции, для которых контроль не включен

DSPCSPOBJ

Показать объект CSP

WRKOBJCSP

Работа с объектами для CSP

Операции над таблицей межсистемных продуктов (*CSPTBL)

В этом списке указаны операции, выполняемые над таблицей межсистемных продуктов (*CSPTBL), и условия их контроля.

- Операция чтения

Справочник

Когда упоминается в приложении CSP

- Операция изменения

Нет

- Операции, для которых контроль не включен

DSPCSPOBJ

Показать объект CSP

WRKOBJCSP

Работа с объектами для CSP

Операции над описанием контроллера (*CTLDD)

В этом списке указаны операции, выполняемые над описанием контроллера (*CTLDD), и условия их контроля.

- Операция чтения

SAVCFG

Сохранить конфигурацию

VFYCMN

Проверка соединения

- Операция изменения

CHGCTLxxx

Изменить описание контроллера

VRFCFG

Включить или выключить описание контроллера

- Операции, для которых контроль не включен

DSPCTLD

Показать описание контроллера

ENDCTLRCY

Прекратить исправление ошибок контроллера

PRTDEVADR

Печать адреса устройства

RSMCTLRCY

Возобновить исправление ошибок контроллера

RTVCFGSRC

Получить исходный текст описания контроллера

RTVCFGSTS

Получить состояние описания контроллера

WRKCTLD

Скопировать описание контроллера

WRKCTLD

Работа с описанием контроллера

Операции над описанием устройства (*DEV D)

В этом списке указаны операции, выполняемые над описанием устройства (*DEV D), и условия их контроля.

- Операция чтения

Захват Первый захват устройства при выполнении операции чтения или явный захват устройства

Выделение

Выделение диалога

SAVCFG

Сохранить конфигурацию

STRPASTHR

Начать сеанс удаленного входа в систему

Запуск второго сеанса для входа в промежуточную систему

VFYCMN

Проверка соединения

- Операция изменения

CHGDEVxxx

Изменить описание устройства

HLDDEVxxx

Блокировать описание устройства

RLSDEVxxx

Разблокировать описание устройства

QWSSETWS

Изменить параметр буферизации ввода для устройства

VRFCFG

Включить или выключить описание устройства

- Операции, для которых контроль не включен

DSPDEV D

Показать описание устройства

DSPMODSTS

Показать состояние режима

ENDDEVRCY

Прекратить исправление ошибок устройства

HLDCMNDEV

Блокировать устройство связи

RLSCMNDEV

Разблокировать устройство связи

RSMDEVRCY

Возобновить исправление ошибок устройства

RTVCFG SRC

Получить исходный текст описания устройства

RTVCFGSTS

Получить состояние описания устройства

WRKCFGSTS

Работа с состоянием устройства

WRKDEVD

Скопировать описание устройства

WRKDEVD

Работа с описанием устройства

Операции над каталогом (*DIR)

| В этом списке указаны операции, выполняемые над каталогом (*DIR), и условия их контроля.

- Операции чтения/поиска

access, accessx, QlgAccess, QlgAccessx

Определить доступные файлы

CHGATR

Изменить атрибут

CPY Скопировать объект

DSPCURDIR

Показать текущий каталог

DSPLNK

Показать ссылки объекта

faccessx

Определить доступные файлы для класса пользователей по дескриптору

getcwd, qlgGetcwd

API Получить полное имя текущего каталога

Qp0lGetAttr, QlgGetAttr

API Получить атрибуты

Qp0lGetPathFromFileID, QlgGetPathFromFileID

API Получить путь из идентификатора файла

Qp0lProcessSubtree, QlgProcessSubtree

API Обработать полное имя

open, open64, QlgOpen, QlgOpen64, Qp0lOpen

API Открыть файл

Qp0lSetAttr, QlgSetAttr

API Задать атрибуты

opendir, QlgOpendir

API Открыть каталог

RTVCURDIR

Получить текущий каталог

SAV Сохранить объекты

WRKLNK

Работа со ссылками

- Операция изменения

CHGATR

Изменить атрибуты

- CHGAUD**
Изменить значение контроля
- CHGAUT**
Изменить права доступа
- CHGOWN**
Изменить владельца
- CHGPGP**
Изменить основную группу
- chmod, QlgChmod**
API Изменить права доступа к файлу
- chown, QlgChown**
API Изменить владельца и группу
- CPY** Скопировать объект
- CRTDIR**
Создать каталог
- fchmod**
API Изменить права доступа к файлу с помощью дескриптора
- fchown**
API Изменить владельца и группу файла с помощью дескриптора
- mkdir, QlgMkdir**
API Создать каталог
- MOV** Переместить объект
- Qp0IRenameKeep, QlgRenameKeep**
API Переименовать файл или каталог, сохранить новый экземпляр
- Qp0IRenameUnlink, QlgRenameUnlink**
API Переименовать файл или каталог, отключить новый экземпляр
- Qp0ISetAttr, QlgSetAttr**
API Задать атрибут
- rmdir, QlgRmdir**
API Удалить каталог
- RMVDIR**
Удалить каталог
- RNM** Переименовать объект
- RST** Восстановить объект
- utime, QlgUtime**
API Задать время изменения файла и обращения к нему
- WRKAUT**
Работа с правами доступа
- WRKLNK**
Работа со ссылками объекта
- Операции, для которых контроль не включен
- chdir, QlgChdir**
API Изменить каталог

CHGCURDIR

Изменить текущий каталог

close API Закрыть дескриптор файла

closedir

API Закрыть каталог

DSPAUT

Показать права доступа

dup API Скопировать дескриптор открытого файла

dup2 API Скопировать дескриптор открытого файла в другой дескриптор

faccessx

Определить доступные файлы для класса пользователей по дескриптору

fchdir Изменить текущий каталог с помощью дескриптора

fcntl API Выполнить команду управления файлами

fpathconf

API Получить настраиваемые переменные полного имени с помощью дескриптора

fstat, fstat64

API Получить информацию о файле с помощью дескриптора

givedescriptor

API Предоставить доступ к файлу

ioctl API Выполнить запрос на управление вводом-выводом

lseek, lseek64

API Задать смещение в файле для чтения/записи

lstat, lstat64, QlgLstat, QlgLstat64

API Получить информацию о файле или связи

pathconf, QlgPathconf

API Получить настраиваемые переменные полного имени

readdir

API Прочитать запись каталога

rewinddir

API Сбросить поток каталога

select API Проверить состояние ввода-вывода нескольких дескрипторов файлов

stat, QlgStat

API Получить информацию о файле

takedescriptor

API Принять права доступа к файлу

Операции с сервером каталогов

В этом списке указаны операции, выполняемые с сервером каталогов, и условия их контроля.

Примечание: Действия сервера каталогов контролируются в том случае, если в системном значении Контроль действий (QAUDLVL) или в параметре пользовательского профайла Контроль действий (AUDLVL) задано значение *OFCSRV.

- Операции, для которых включен контроль

Добавление

Добавление записей каталога

Изменение

Изменение сведений о записях каталога

Удаление

Удаление записей каталога

Переименование

Переименование записей каталога

Печать

Просмотр или печать сведений о записях каталога

Просмотр или печать сведений об отделе

Просмотр или печать записей каталога, полученных в результате поиска

RTVDIRE

Получить запись каталога

Собрать

Сбор данных о записях каталога путем теневого копирования каталога

Получить

Получение данных о записях каталога с помощью теневого копирования

- Операции, для которых контроль не включен

Команды CL

Для контроля за отдельными командами CL, предназначенными для работы с каталогом, можно включить функцию контроля за объектами.

Примечание: При выполнении некоторых команд CL для работы с каталогом контрольная запись все же создается, поскольку эти команды выполняют функции, относящиеся к уровню контроля *OFCSRV, например, добавляют запись каталога.

CHGSYSDIRA

Изменить атрибуты системного каталога

Отделы

Добавление, изменение, удаление и просмотр данных об отделах каталога

Описания

Присвоение описания записи каталога с помощью опции 8 меню WRKDIR.

Добавление, изменение и удаление описаний записей каталога

Списки рассылки

Добавление, изменение, переименование и удаление списков рассылки

ENDDIRSHD

Прекратить теневое копирование каталога

Просмотр списка

Просмотр и печать списка записей каталога, не содержащего сведения о записях. Например, такой список можно получить введя команду WRKDIR или выбрав записи для отправки записки с помощью клавиши F4.

Географические объекты

Добавление, изменение, удаление и просмотр данных о расположении каталога

Псевдоним

Добавление, изменение, переименование и удаление псевдонимов

Поиск Поиск записей каталога

STRDIRSHD

Начать теневое копирование каталога

Операции над объектом библиотеки документов (*DOC или *FLR)

В этом списке указаны операции, выполняемые над объектом библиотеки документов (*DOC или *FLR), и условия их контроля.

- Операция чтения

CHKDOC

Проверить правописание в документе

CPYDOC

Скопировать документ

DMPDLO

Создать дамп DLO

DSPDLOAUD

Показать параметры контроля DLO

Примечание: Если для папки включена функция контроля за объектом, то при просмотре информации о контроле для всех документов папки создается контрольная запись. При просмотре информации о контроле для отдельных документов папки контрольная запись не создается.

DSPDLOAUT

Показать права доступа к DLO

DSPDOC

Показать документ

DSPHLPDOC

Показать справочный документ

EDTDLOAUT

Редактировать права доступа к DLO

MRGDOC

Вставить документ

PRTDOC

Печать документа

QHFCPYSF

API Скопировать потоковый файл

QHFGETSZ

API Получить размер потокового файла

QHFRDDR

API Прочитать запись каталога

QHFRDSF

API Прочитать потоковый файл

RTVDOC

Загрузить документ

SAVDLO

Сохранить DLO

SAVSHF

Сохранить книжную полку

SNDDOC
Отправить документ

SNDDST
Отправить рассылку

WRKDOC
Работа с документом

Примечание: Создается запись о чтении папки, содержащей документы.

- Операция изменения

ADDLOAUT
Добавить права доступа к DLO

ADDOFCENR
Добавить регистрацию в Office

CHGDLOAUD
Изменить параметры контроля DLO

CHGDLOAUT
Изменить права доступа к DLO

CHGDLOOWN
Изменить права доступа к DLO

CHGDLOPGP
Изменить основную группу DLO

CHGDOCD
Изменить описание документа

CHGDSTD
Изменить описание рассылки

CPYDOC²
Скопировать документ

Примечание: Если целевой документ уже существует, то создается запись об изменении.

CRTFLR
Создать папку

CVTTOFLR²
Преобразовать в папку

DLTDLO²
Удалить DLO

DLTSHF
Удалить книжную полку

DTLDOCL²
Удалить список документов

DLTDST²
Удалить рассылку

EDTDLOAUT
Редактировать права доступа к DLO

2. Если целевой объект расположен в папке, то запись об изменении создается как для документа, так и для папки.

EDTDOC

Редактировать документ

FILDOC ²

Зарегистрировать документ

GRTACCAUT

Предоставить права доступа к коду доступа

GRTUSRPMN

Предоставить права доступа пользователю

MOVDOC ²

Переместить документ

MRGDOC ²

Вставить документ

PAGDOC

Разбить документ на страницы

QHFCHGAT

API Изменить атрибуты записи каталога

QHFSETSZ

API Задать размер потокового файла

QHFWRTSF

API Записать данные в потоковый файл

QRYDOCLIB ²

Запросить библиотеку документов

Примечание: При замене документа, полученного в результатах поиска, создается запись об изменении.

RCVDST ²

Получить рассылку

RGZDLO

Реорганизовать DLO

RMVACC

Удалить код доступа для всех DLO, с которыми связан этот код

RMVDLOAUT

Удалить права доступа к DLO

RNMDLO ²

Переименовать DLO

RPLDOC

Заменить документ

RSTDLO ²

Восстановить DLO

RSTSHF

Восстановить книжную полку

RTVDOC

Получить документ (изъять)

RVKACCAUT

Аннулировать права доступа к коду доступа

RVKUSRPMN

Аннулировать права доступа пользователя

SAVDLO²

Сохранить DLO

- Операции, для которых контроль не включен

ADDACC

Добавить код доступа

DSPACC

Показать код доступа

DSPUSRPMN

Показать права доступа пользователя

QHFCHGFP

API Изменить указатель файла

QHFCLODR

API Закрыть каталог

QHFCLOSF

API Закрыть потоковый файл

QHFFRCSF

API Принудительно отправить буферизованные данные

QHFLULSF

API Блокировать/разблокировать диапазон в потоковом файле

QHFRTVAT

API Получить атрибуты записи каталога

RCLDLO

Восстановить DLO (*ALL или *INT)

WRKDOCLIB

Работа с библиотекой документов

WRKDOCPRTQ

Работа с очередью печати документов

Операции над областью данных (*DTAARA)

В этом списке указаны операции, выполняемые над областью данных (*DTAARA), и условия их контроля.

- Операция чтения

DSPDTAARA

Показать область данных

RCVDTAARA

Принять область данных (команда S/38)

RTVDTAARA

Получить область данных

QWCRDTAA

API Получить область данных

- Операция изменения

CHGDTAARA

Изменить область данных

SNDDTAARA

Отправить область данных

- Операции, для которых контроль не включен

Области данных

Локальная область данных, групповая область данных, область данных PIP (параметров инициализации программы)

WRKDTAARA

Работа с областями данных

Операции в Утилите интерактивного определения данных (*DTADCT)

В этом списке указаны операции, выполняемые в Утилите интерактивного определения данных (*DTADCT), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

Создание

Словарь данных и определения данных

Изменение

Словарь данных и определения данных

Копирование

Определения данных (фиксируется так же, как и операция создания)

Удаление

Словарь данных и определения данных

Переименование

Определения данных

- Операции, для которых контроль не включен

Просмотр

Словарь данных и определения данных

LNKDTADFN

Подключение и отключение определений файлов

Печать

Словарь данных, определения данных и информация об области применения определений данных

Операции над очередью данных (*DTAQ)

В этом списке указаны операции, выполняемые над очередью данных (*DTAQ), и условия их контроля.

- Операция чтения

QMHRDQM

API Получить сообщение из очереди данных

- Операция изменения

QRCVDTAQ

API Получить очередь данных

QSNDDTAQ

API Отправить очередь данных

QCLRDTAQ

API Очистить очередь данных

- Операции, для которых контроль не включен

WRKDTAQ

Работа с очередью данных

QMHQRDQD

API Получить описание очереди данных

Операции над описанием формата (*EDTD)

В этом списке указаны операции, выполняемые над описанием формата (*EDTD), и условия их контроля.

- Операция чтения

DSPEDTD

Показать описание формата

QECCVTEC

API Расширение кода форматирования (через процедуру QECEDITU)

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKEDTD

Работа с описаниями формата

QECEDT

API Форматирование

QECCVTEW

API для преобразования операции форматирования в маску форматирования

Операции над записями регистрации точек выхода (*EXITRG)

В этом списке указаны операции, выполняемые над записями регистрации точек выхода (*EXITRG), и условия их контроля.

- Операция чтения

QUSRTVEI

API Получить информацию о точке выхода

QusRetrieveExitInformation

API Получить информацию о точке выхода

- Операция изменения

ADDEXITPGM

Добавить программу выхода

QUSADDEP

API Добавить программу выхода

QusAddExitProgram

API Добавить программу выхода

QUSDRGPT

API Отменить регистрацию точки выхода

QusDeregisterExitPoint

API Отменить регистрацию точки выхода

QUSRGPT

API Зарегистрировать точку выхода

QusRegisterExitPoint

API Зарегистрировать точку выхода

QUSRMVEP

API Удалить программу выхода

QusRemoveExitProgram

API Удалить программу выхода

RMVEXITPGM

Удалить программу выхода

WRKREGINF

Работа с регистрационной информацией

- Операции, для которых контроль не включен

Нет

Операции над таблицей управления формами (*FCT)

В этом списке указаны операции, выполняемые над таблицей управления формами (*FCT), и условия их контроля.

- Никакие операции чтения и изменения объектов типа *FCT не контролируются.

Операции над файлами (*FILE)

В этом списке указаны операции, выполняемые над файлами (*FILE), и условия их контроля.

- Операция чтения

SPYF Скопировать файл (использует операцию открытия)

Открытие

Открыть файл для чтения

DSPPFM

Показать элемент физического файла (использует операцию открытия)

Открытие

Открыть MRT после первоначального открытия

CRTBSCF

Создать файл BSC (использует операцию открытия)

CRTCMNF

Создать файл средств связи (использует операцию открытия)

CRTDSPF

Создать файл дисплея (использует операцию открытия)

CRTICFF

Создать файл ICF (использует операцию открытия)

CRTMXDF

Создать файл MXD (использует операцию открытия)

CRTPRTF

Создать файл принтера (использует операцию открытия)

CRTPF

Создать физический файл (использует операцию открытия)

CRTL

Создать логический файл (использует операцию открытия)

DSPMODSRC

Показать исходный текст модуля (использует операцию открытия)

STRDBG

Начать отладку (использует операцию открытия)

QTEDBGS

API Получить текст представления

- Операция изменения

Открытие

Открыть файл для изменения

ADDBSCDEVE

(S/38E) Добавить запись о бисинхронном устройстве в смешанный файл устройств

ADDCMNDEVE

(S/38E) Добавить запись об устройстве средств связи в смешанный файл устройств

ADDDSPDEVE

(S/38E) Добавить запись о дисплейном устройстве в смешанный файл устройств

ADDICFDEVE

(S/38E) Добавить запись об устройстве ICF в смешанный файл устройств

ADDLFM

Добавить элемент логического файла

ADDPFCST

Добавить ограничение для физического файла

ADDPFM

Добавить элемент физического файла

ADDPFTRG

Добавить триггер для физического файла

ADDPFVLM

Добавить элемент переменной длины в физический файл

APYJRNCHGX

Применить дополнительно зарегистрированные изменения

CHGBSCF

Изменить функцию бисинхронной связи

CHGCMNF

(S/38E) Изменить файл средств связи

CHGDDMF

Изменить файл DDM

CHGDKTF

Изменить файл дискеты

CHGDSPF

Изменить файл дисплея

CHGICFDEVE

Изменить запись файла устройств ICF

CHGICFF

Изменить файл ICF

CHGMXDF
(S/38E) Изменить смешанный файл устройств

CHGLF
Изменить логический файл

CHGLFM
Изменить элемент логического файла

CHGPF
Изменить физический файл

CHGPFCST
Изменить ограничение для физического файла

CHGPFM
Изменить элемент физического файла

CHGPRTF
Изменить GQle принтера

CHGSAVF
Изменить файл сохранения

CHGS36PRCA
Изменить атрибуты процедуры S/36

CHGS36SRCA
Изменить атрибуты исходного текста S/36

CHGTAPF
Изменить файл лентопротяжного устройства

CLRPFM
Очистить элемент физического файла

CPYF Скопировать файл (открыть файл для изменения, например добавления записей, очистки элемента или сохранения элемента)

EDTS36PRCA
Редактировать атрибуты процедуры S/36

EDTS36SRCA
Редактировать атрибуты исходного текста S/36

INZPFM
Инициализировать элемент физического файла

JRNAP
(S/38E) Начать ведение журнала пути доступа (одна запись для каждого файла)

JRNPF
(S/38E) Начать ведение журнала физического файла (одна запись для каждого файла)

RGZPFM
Реорганизовать элемент физического файла

RMVBSCDEVE
(S/38E) Удалить запись об устройстве BSC из смешанного файла устройств

RMVCMNDEVE
(S/38E) Удалить запись об устройстве CMN из смешанного файла устройств

RMVDSPDEVE
(S/38E) Удалить запись об устройстве DSP из смешанного файла устройств

RMVICFDEVE
(S/38E) Удалить запись об устройстве ICF из файла устройств ICM

RMVM
Удалить элемент

RMVPFCST
Удалить ограничение для физического файла

RMVPFTGR
Удалить триггер для физического файла

RNMM
Переименовать элемент

WRKS36PRCA
Работа с атрибутами процедуры S/36

WRKS36SRCA
Работа с атрибутами исходного текста S/36

- Операции, для которых контроль не включен

| **CHGPFTRG**
| Изменить триггер для физического файла

DSPCPCST
Показать ограничения, ожидающие проверки

DSPFD
Показать описание файла

DSPFFD
Показать описание полей файла

DSPDBR
Показать связи базы данных

DSPPGMREF
Показать ссылки на файл программы

EDTCPCST
Изменить ограничения, ожидающие проверки

OVRxxx
Переопределить файл

RTVMBRD
Получить описание элемента

WRKPCST
Работа с ограничениями физического файла

WRKF
Работа с файлами

Операции над файлами FIFO (*FIFO)

В этом списке указаны операции, выполняемые над файлами FIFO (*FIFO), и условия их контроля.

Информация о контроле за объектами *FIFO приведена в разделе Операции над потоковым файлом (*STMF).

Операции над папкой (*FLR)

В этом списке указаны операции, выполняемые над папкой (*FLR), и условия их контроля.

См. раздел “Операции над объектом библиотеки документов (*DOC или *FLR)” на стр. 544

Операции над ресурсом шрифта (*FNTRSC)

В этом списке указаны операции, выполняемые над ресурсом шрифта (*FNTRSC), и условия их контроля.

- Операция чтения

Печать

Печать буферного файла, ссылающегося на ресурс шрифта

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKFNTRSC

Работа с ресурсами шрифтов

Печать

В том случае, если при создании буферного файла использовался ресурс шрифта

Операции над определением формы (*FORMDF)

В этом списке указаны операции, выполняемые над определением формы (*FORMDF), и условия их контроля.

- Операция чтения

Печать

Печать буферного файла, использующего определение формы

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKFORMDF

Работа с определениями форм

Печать

В том случае, если при создании буферного файла использовалось определение формы

Операции над объектом фильтра (*FTR)

В этом списке указаны операции, выполняемые над объектом фильтра (*FTR), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

ADDALRACNE

Добавить запись о действии при получении предупреждения

ADDALRSLTE

Добавить запись о выборе предупреждений

ADDPRBACNE

Добавить запись о действии в случае неполадки

ADDPBLSLTE

Добавить запись о выборе неполадок

CHGALRACNE

Изменить запись о действии при получении предупреждения

CHGALRSLTE

Изменить запись о выборе предупреждений

CHGPRBACNE

Изменить запись о действии в случае неполадки

CHGPRBSLTE

Изменить запись о выборе неполадок

CHGFTR

Изменить фильтр

RMVFTRACNE

Удалить запись о действии при получении предупреждения

RMVFTRSLTE

Удалить запись о выборе предупреждений

WRKFTRACNE

Работа с записью о действии при получении предупреждения

WRKFTRSLTE

Работа с записью о выборе предупреждений

- Операции, для которых контроль не включен

WRKFTR

Работа с фильтром

WRKFTRACNE

Работа с записями о действиях фильтра

WRKFTRSLTE

Работа с записями о выборе фильтра

Операции над набором графических символов (*GSS)

В этом списке указаны операции, выполняемые над набором графических символов (*GSS), и условия их контроля.

- Операция чтения

Загружен

Когда набор загружен

Шрифт

Когда набор применяется в качестве шрифта во внешне описанном файле принтера

- Операция изменения

Нет.

- Операции, для которых контроль не включен

WRKGSS

Работа с набором графических символов

Операции над словарем набора двухбайтовых символов (*IGCDCT)

В этом списке указаны операции, выполняемые над словарем набора двухбайтовых символов (*IGCDCT), и условия их контроля.

- Операция чтения

DSPIGCDCT

Показать словарь IGC

- Операция изменения

EDTIGCDCT

Редактировать словарь IGC

Операции над сортировкой набора двухбайтовых символов (*IGCSRT)

В этом списке указаны операции, выполняемые над сортировкой набора двухбайтовых символов (*IGCSRT), и условия их контроля.

- Операция чтения

SPYIGCSRT

Скопировать сортировку IGC (*исходный-объект-**IGCSRT)

Преобразование

Преобразование в формат V3R1, если это необходимо

Печать

Печать символа для регистрации в таблице сортировки (опция 1 меню CGU)

Печать перед удалением символа из таблицы сортировки (опция 2 меню CGU)

- Операция изменения

SPYIGCSRT

Скопировать сортировку IGC (*целевой-объект-**IGCSRT)

Преобразование

Преобразование в формат V3R1, если это необходимо

Создание

Создать пользовательский символ (опция 1 меню CGU)

Удаление

Удалить пользовательский символ (опция 2 меню CGU)

Обновление

Обновить активную таблицу сортировки (опция 5 меню CGU)

- Операции, для которых контроль не включен

FMTDTA

Записи сортировки или поля файла

Операции над таблицей набора двухбайтовых символов (*IGCTBL)

В этом списке указаны операции, выполняемые над таблицей набора двухбайтовых символов (*IGCTBL), и условия их контроля.

- Операция чтения

SPYIGCTBL

Скопировать таблицу IGC

STRFMA

Запустить средство управления шрифтами

- Операция изменения

STRFMA

Запустить средство управления шрифтами

- Операции, для которых контроль не включен

CHKIGCTBL

Проверить таблицу IGC

Операции над описанием задания (*JOBQ)

В этом списке указаны операции, выполняемые над описанием задания (*JOBQ), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

CHGJOBQ

Изменить описание задания

- Операции, для которых контроль не включен

DSPJOBQ

Показать описание задания

WRKJOBQ

Работа с описанием задания

QWDRJOBQ

API Получить описание задания

Пакетное задание

Когда применяется для установки задания

Операции над очередью заданий (*JOBQ)

В этом списке указаны операции, выполняемые над очередью заданий (*JOBQ), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

Запись При добавлении или удалении записи очереди

CHGJOBQ

Изменить очередь заданий

CLRJOBQ

Очистить очередь заданий

HLDJOBQ

Блокировать очередь заданий

RLSJOBQ

Разблокировать очередь заданий

- Операции, для которых контроль не включен

ADDJOBQE “Описания подсистем” на стр. 215

Добавить запись очереди заданий

CHGJOB

Переместить задание из одной JOBQ в другую JOBQ

CHGJOBQE “Описания подсистем” на стр. 215

Изменить запись очереди заданий

QSPRJOBQ

Получить информацию об очереди заданий

RMVJOBQE “Описания подсистем” на стр. 215

Удалить запись очереди заданий

TFRJOB

Перейти к заданию

TFRVCHJOB

Перейти к пакетному заданию

WRKJOBQ

Работа с конкретной очередью заданий

WRKJOBQ

Работа со всеми очередями заданий

WRKJOBQD

Работа с описанием очереди задания

Операции над планировщиком заданий (*JOBSCD)

В этом списке указаны операции, выполняемые над планировщиком заданий (*JOBSCD), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

ADDJOBSCDE

Добавить запись расписания заданий

CHGJOBSCDE

Изменить запись расписания заданий

RMVJOBSCDE

Удалить запись расписания заданий

HLDJOBSCDE

Блокировать запись расписания заданий

RLSJOBSCDE

Разблокировать запись расписания заданий

- Операции, для которых контроль не включен

Просмотр

Показать сведения о запланированном задании

WRKJOBSCDE

Работа с записями расписания заданий

Работа с ...

Работа с заданиями из записи расписания, уже переданными на выполнение

3. Если функция контроля за объектом включена для описания подсистемы (*SBSD), то контрольная запись будет создана.

QWCLSCDE

API Показать запись расписания заданий

Операции над журналом (*JRN)

В этом списке указаны операции, выполняемые над журналом (*JRN), и условия их контроля.

- Операция чтения

CMPJRNIMG

Сравнить образы журнала

DSPJRN

Показать запись журнала (для пользовательских журналов)

QJORJIDI

Получить информацию об идентификаторе журнала (JID)

QjoRetrieveJournalEntries

Получить записи журнала

RCVJRNE

Принять запись журнала

RTVJRNE

Получить запись журнала

- Операция изменения

ADDRMTJRN

Добавить удаленный журнал

APYJRNCHG

Применить зарегистрированные изменения

APYJRNCHGX

Применить дополнительно зарегистрированные изменения

CHGJRN

Изменить журнал

CHGRMTJRN

Изменить удаленный журнал

ENDJRNxxx

Завершить ведение журнала

JRNAP

(S/38E) Начать ведение журнала пути доступа

JRNPF

(S/38E) Начать ведение журнала физического файла

QjoAddRemoteJournal

API Добавить удаленный журнал

QjoChangeJournalState

API Изменить состояние журнала

QjoEndJournal

API Завершить ведение журнала

QjoRemoveRemoteJournal

API Удалить удаленный журнал

QJOSJRNE

API Отправить запись журнала (только при отправке пользовательских записей с помощью API QJOSJRNE)

QjoStartJournal

API Начать ведение журнала

RMVJRNCHG

Удалить зарегистрированные изменения

RMVRMTJRN

Удалить удаленный журнал

SNDJRNE

Отправить запись журнала (только при отправке пользовательских записей с помощью команды SNDJRNE)

STRJRNxxx

Начать ведение журнала

- Операции, для которых контроль не включен

DSPJRN

Показать запись журнала для внутренних системных журналов, JRN(*INTSYSJRN)

DSPJRNA

(S/38E) Работа с атрибутами журнала

DSPJRNMNU

(S/38E) Работа с журналом

QjoRetrieveJournalInformation

API Получить информацию о журнале

WRKJRN

Работа с журналом (в среде S/38 - DSPJRNMNU)

WRKJRNA

Работа с атрибутами журнала (в среде S/38 - DSPJRNA)

Операции над получателем журнала (*JRNRCV)

В этом списке указаны операции, выполняемые над получателем журнала (*JRNRCV), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

CHGJRN

Изменить журнал (при подключении новых получателей)

- Операции, для которых контроль не включен

DSPJRNRCVA

Показать атрибуты получателя журнала

QjoRtvJrnReceiverInformation

Получить информацию о получателе журнала, API

WRKJRNRCV

Работа с получателем журнала

Операции над библиотекой (*LIB)

В этом списке указаны операции, выполняемые над библиотекой (*LIB), и условия их контроля.

- Операция чтения

DSPLIB

Показать библиотеку (если библиотека не пуста. Если библиотека пуста, контрольная запись не создается.)

Найти При поиске объекта в библиотеке.

Примечание:

1. Для одной команды работы с библиотекой может быть создано несколько контрольных записей. Например, при открытии файла в журнал контроля заносится запись о библиотеке для самого файла и всех его элементов.
2. Если файл найти не удалось, то контрольная запись не создается. Например, предположим, что была вызвана следующая команда с шаблонами имен:
DSPOBJD OBJ(AR/WRK*) OBJTYPE(*FILE)
Если библиотека “AR” не содержит ни одного файла, имя которого начинается с “WRK”, то контрольная запись для этой библиотеки создана не будет.

Список библиотек

Добавление библиотеки в список

- Операция изменения

CHGLIB

Изменить библиотеку

CLRLIB

Очистить библиотеку

MOVOBJ

Переместить объект

RNMOBJ

Переименовать объект

Добавление

Добавить объект в библиотеку

Удаление

Удалить объект из библиотеки

- Операции, для которых контроль не включен

Нет

Операции над описанием линии (*LIND)

В этом списке указаны операции, выполняемые над описанием линии (*LIND), и условия их контроля.

- Операция чтения

SAVCFG

Сохранить конфигурацию

RUNLPDA

Выполнить операционную команду LPDA-2

VFYCMN

Проверка соединения

VFYLNKLPDA

Проверить линию связи LPDA-2

- Операция изменения

CHGLINxxx

Изменить описание линии

VRFCFG

Включить или выключить описание линии

- Операции, для которых контроль не включен

ANSLIN

Линия - Ответ

Копирование

Опция 3 меню WRKLIND

DSPLIND

Показать описание линии

ENDLINRCY

Прекратить исправление ошибок линии

RLSCMNDEV

Разблокировать устройство связи

RSMLINRCY

Возобновить исправление ошибок линии

RTVCFGSRC

Получить исходный текст описания линии

RTVCFGSTS

Получить состояние описания линии

WRKLIND

Работа с описаниями линий

WRKCFGSTS

Работа с состоянием описания линии

Операции над почтовыми службами

В этом списке указаны операции, выполняемые над почтовыми службами, и условия их контроля.

Примечание: Действия почтовых служб контролируются в том случае, если в системном значении Контроль действий (QAUDLVL) или в параметре пользовательского профайла Контроль действий (AUDLVL) задано значение *OFCSRV.

- Операции, для которых включен контроль

Изменение

Переход в системный каталог рассылки

Работа от имени

Работа от имени другого пользователя

Примечание: Работа от имени другого пользователя контролируется только в том случае, если в параметре AUDLVL пользовательского профайла или в системном значении QAUDLVL задано значение *SECURITY.

Открытие

При открытии почтового протокола создается контрольная запись

- Операции, для которых контроль не включен

Изменение

Изменить сведения о почтовом сообщении

Удаление

Удалить почтовое сообщение

Файл Поместить почтовое сообщение в документ или папку

Примечание: Почтовое сообщение, помещенное в документ или папку, становится объектом библиотеки документов (DLO). Для DLO можно включить контроль за объектом.

Переслать

Переслать почтовое сообщение

Печать

Печать почтового сообщения.

Примечание: Для контроля за печатью почтовых сообщений можно установить уровень контроля *SPLFDTA или *PRTDTA.

Получение

Получить почтовое сообщение

Ответить

Ответить на почтовое сообщение

Отправка

Отправить почтовое сообщение

Вид Показать почтовое сообщение

Операции над меню (*MENU)

В этом списке указаны операции, выполняемые над меню (*MENU), и условия их контроля.

- Операция чтения

Просмотр

Просмотр меню с помощью команды GO MENU или команды окна диалога UIM

- Операция изменения

CHGMNU

Изменить меню

- Операции, для которых контроль не включен

Возврат

Возврат к одному из ранее просмотренных меню

DSPMNUA

Показать атрибуты меню

WRKMNU

Работа с меню

Операции над описанием режима (*MODD)

В этом списке указаны операции, выполняемые над описанием режима (*MODD), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

CHGMODD

Изменить описание режима

- Операции, для которых контроль не включен

CHGSSNMAX

Изменить максимальное число сеансов

DSPMODD

Показать описание режима

ENDMOD

Выключить режим

STRMOD

Включить режим

WRKMODD

Работа с описаниями режимов

Операции над объектом модуля (*MODULE)

В этом списке указаны операции, выполняемые над объектом модуля (*MODULE), и условия их контроля.

- Операция чтения

CRTPGM

При выполнении команды CRTPGM создается контрольная запись для каждого модуля.

CRTSRVPGM

При выполнении команды CRTSRVPGM создается контрольная запись для каждого модуля.

UPDPGM

При выполнении команды UPDPGM создается контрольная запись для каждого модуля.

UPDSRVPGM

При выполнении команды UPDSRVPGM создается контрольная запись для каждого модуля.

- Операция изменения

CHGMOD

Изменить модуль

- Операции, для которых контроль не включен

DSPMOD

Показать модуль

RTVBNSRC

Получить исходный файл редактора связей

WRKMOD

Работа с модулем

Операции над файлом сообщений (*MSGF)

В этом списке указаны операции, выполняемые над файлом сообщений (*MSGF), и условия их контроля.

- Операция чтения

DSPMSGD

Показать описание сообщения

MRGMSGF

Вставить файл сообщений исходный-файл

Печать

Печать описания сообщения

RTVMSG

Получить информацию из файла сообщений

QMHRVTVM

API Получить сообщение

WRKMSGD

Работа с описанием сообщения

- Операция изменения

ADDMSGD

Добавить описание сообщения

CHGMSGD

Изменить описание сообщения

CHGMSGF

Изменить файл сообщений

MRGMSGF

Вставить файл сообщений (целевой-файл и MSGF замещения)

RMVMSGD

Удалить описание сообщения

- Операции, для которых контроль не включен

OVRMSGF

Переопределить файл сообщений

WRKMSGF

Работа с файлом сообщений

QMHRMFAT

API Получить атрибуты файла сообщений

Операции над очередью сообщений (*MSGQ)

В этом списке указаны операции, выполняемые над очередью сообщений (*MSGQ), и условия их контроля.

- Операция чтения

QMHLSM

API Показать сообщения, отличные от сообщений программы

QMHRMQAT

API Получить атрибуты очереди сообщений, отличных от сообщений программы

DSPLOG

Показать протокол

DSPMSG

Показать сообщение

Печать

Печать сообщений

RCVMSG

Получить сообщение RMV(*NO)

QMHRMCM

API Получить сообщения, отличные от сообщений программы, если действие над сообщением не равно *REMOVE.

- Операция изменения

CHGMSGQ

Изменить очередь сообщений

CLRMSGQ

Очистить очередь сообщений

RCVMSG

Получить сообщение RMV(*YES)

QMHRMVM

API Получить сообщения, отличные от сообщений программы, если действие над сообщением равно *REMOVE.

RMVMSG

Удалить сообщение

QMHRMVM

API Удалить сообщения, отличные от сообщений программы

SNDxxxMSG

Отправить сообщение в очередь

QMHSNDBM

API Отправить прерывающее сообщение

QMHSNDM

API Отправить непрограммное сообщение

QMHSNDRM

API Отправить ответное сообщение

SNDRPY

Отправить ответ

WRKMSG

Работа с сообщением

- Операции, для которых контроль не включен

WRKMSGQ

Работа с очередью сообщений

Программа

Операции над очередью сообщений программы

Операции над группой узлов (*NODGRP)

В этом списке указаны операции, выполняемые над группой узлов (*NODGRP), и условия их контроля.

- Операция чтения

DSPNODGRP

Показать группу узлов

- Операция изменения

CHGNODGRPA

Изменить группу узлов

Операции над списком узлов (*NODL)

В этом списке указаны операции, выполняемые над списком узлов (*NODL), и условия их контроля.

- Операция чтения

QFVLSTNL

Показать записи списка узлов

- Операция изменения
ADDNODLE
Добавить запись списка узлов
- Операция изменения
RMVNODLE
Удалить запись списка узлов
- Операции, для которых контроль не включен
WRKNODL
Работа со списком узлов
- Операции, для которых контроль не включен
WRKNODLE
Работа с записями списка узлов

Операции над описанием NetBIOS (*NTBD)

В этом списке указаны операции, выполняемые над описанием NetBIOS (*NTBD), и условия их контроля.

- Операция чтения
SAVCFG
Сохранить конфигурацию
- Операция изменения
CHGNTBD
Изменить описание NetBIOS
- Операции, для которых контроль не включен
Копирование
Опция 3 меню WRKNTBD
- Операции, для которых контроль не включен
DSPNTBD
Показать описание NetBIOS
- Операции, для которых контроль не включен
RTVCFGSRC
Получить исходный текст описания NetBIOS
- Операции, для которых контроль не включен
WRKNTBD
Работа с описанием NetBIOS

Операции над сетевым интерфейсом (*NWID)

В этом списке указаны операции, выполняемые над сетевым интерфейсом (*NWID), и условия их контроля.

- Операция чтения
SAVCFG
Сохранить конфигурацию
- Операция изменения
CHGNWIISDN
Изменить описание сетевого интерфейса
- Операции, для которых контроль не включен
VRFCFG
Включить или выключить описание сетевого интерфейса
- Операции, для которых контроль не включен
Копирование
Опция 3 меню WRKNWID
- Операции, для которых контроль не включен
DSPNWID
Показать описание сетевого интерфейса

ENDNWIRCY

Прекратить исправление ошибок сетевого интерфейса

RSMNWIRCY

Возобновить исправление ошибок сетевого интерфейса

RTVCFGSRC

Получить исходный текст описания сетевого интерфейса

RTVCFGSTS

Получить состояние описания сетевого интерфейса

WRKNWID

Работа с описанием сетевого интерфейса

WRKCFGSTS

Работа с состоянием описания сетевого интерфейса

Операции над описанием сетевого сервера (*NWSD)

В этом списке указаны операции, выполняемые над описанием сетевого сервера (*NWSD), и условия их контроля.

- Операция чтения

SAVCFG

Сохранить конфигурацию

- Операция изменения

CHGNWSD

Изменить описание сетевого сервера

VRFCFG

Изменить состояние конфигурации

- Операции, для которых контроль не включен

Копирование

Опция 3 меню WRKNWSD

DSPNWSD

Показать описание сетевого сервера

RTVCFGSRC

Получить исходный текст конфигурации *NWSD

RTVCFGSTS

Получить состояние конфигурации *NWSD

WRKNWSD

Работа с описанием сетевого сервера

Операции над очередью вывода (*OUTQ)

В этом списке указаны операции, выполняемые над очередью вывода (*OUTQ), и условия их контроля.

- Операция чтения

STRPRTWTR

Запустить загрузчик принтера для OUTQ

STRRMWTR

Запустить удаленный загрузчик для OUTQ

- Операция изменения

Помещение в очередь

При добавлении или удалении записи очереди

CHGOUTQ

Изменить очередь вывода

CHGSPLFA⁴

Изменить атрибуты буферного файла, если файл перемещается в другую очередь вывода, и для старой или новой очереди вывода включен контроль за объектом

CLRROUTQ

Очистить очередь вывода

DLTSPLF⁴

Удалить буферный файл

HLROUTQ

Блокировать очередь вывода

RLSOUTQ

Разблокировать очередь вывода

- Операции, для которых контроль не включен

CHGSPLFA⁴

Изменить атрибуты буферного файла

CPYSPLF⁴

Скопировать буферный файл

Создать⁴

Создать буферный файл

DSPSPLF⁴

Показать буферный файл

HLDSPLF⁴

Блокировать буферный файл

QSPROUTQ

Получить информацию об очереди вывода

RLSSPLF⁴

Разблокировать буферный файл

SNDNETSPLF⁴

Отправить буферный файл по сети

WRKOUTQ

Работа с очередью вывода

WRKOUTQD

Работа с описанием очереди вывода

WRKSPLF

Работа с буферным файлом

WRKSPLFA

Работа с атрибутами буферного файла

Операции над перекрытием (*OVL)

В этом списке указаны операции, выполняемые над перекрытием (*OVL), и условия их контроля.

- Операция чтения

Печать

Печать буферного файла, использующего перекрытие

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKOVL

Работа с перекрытием

Печать

Если при создании буферного файла была задана ссылка на перекрытие

Операции над определением страницы (*PAGDFN)

В этом списке указаны операции, выполняемые над определением страницы (*PAGDFN), и условия их контроля.

- Операция чтения

Печать

Печать буферного файла, ссылающегося на определение страницы

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKPAGDFN

Работа с определением страницы

Печать

В том случае, если при создании буферного файла использовалось определение формы

Операции над сегментом страницы (*PAGSEG)

В этом списке указаны операции, выполняемые над сегментом страницы (*PAGSEG), и условия их контроля.

- Операция чтения

Печать

Печать буферного файла, ссылающегося на сегмент страницы

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKPAGSEG

Работа с сегментом страницы

Печать

В том случае, если при создании буферного файла использовался сегмент страницы

4. Эти операции контролируются, если в параметре контроля действий (системном значении QAUDLVL или параметре пользовательского профайла AUDLVL) задано значение *SPLFDTA.

Операции над группой дескрипторов печати (*PDG)

В этом списке указаны операции, выполняемые над группой дескрипторов печати (*PDG), и условия их контроля.

- Операция чтения

Открытие

При открытии группы дескрипторов печати для чтения с помощью API PrintManager или команды CPI.

- Операция изменения

Открытие

При открытии группы дескрипторов печати для изменения с помощью API PrintManager* или команды CPI.

- Операции, для которых контроль не включен

CHGPDGPRF

Изменить профайл группы дескрипторов печати

WRKPDG

Работа с группой дескрипторов печати

Операции над программой (*PGM)

В этом списке указаны операции, выполняемые над программой (*PGM), и условия их контроля.

- Операция чтения

Активация

Активация программы

Вызов Вызов активированной программы

ADDPGM

Добавить программу для отладки

QTEDBGS

API Qte Зарегистрировать представление отладки

QTEDBGS

API Qte Получить представления модулей

// **RUN** Выполнить программу в среде S/36

RTVCLSRC

Получить исходный текст на CL

STRDBG

Начать отладку

- Операция создания

CRTPGM

Создать программу

UPDPGM

Обновить программу

- Операция изменения

CHGCSPPGM

Изменить программу CSP/AE

CHGPGM

Изменить программу

CHGS36PGMA

Изменить атрибуты программы S/36

EDTS36PGMA

Редактировать атрибуты программы S/36

WRKS36PGMA

Работа с атрибутами программы S/36

- Операции, для которых контроль не включен

ANZPGM

Анализировать программу

DMPCLPGM

Создать дампы программы на CL

DSPCSPOBJ

Показать объект CSP

DSPPGM

Показать программу

PRTCMDUSG

Печать формата команды

PRTCSPAPP

Печать приложения CSP

PRTSQLINF

Печать информации SQL

QBNLPGMI

API Показать информацию о программе ILE

QCLRPGMI

API Получить информацию о программе

STRCSP

Запустить утилиты CSP

TRCCSP

Трассировать приложение CSP

WRKOBJCSP

Работа с объектами для CSP

WRKPGM

Работа с программой

Операции над группой панелей (*PNLGRP)

В этом списке указаны операции, выполняемые над группой панелей (*PNLGRP), и условия их контроля.

- Операция чтения

ADDSCHIDX

Добавить запись индекса поиска

QUIOPNDA

API Открыть группу панелей для просмотра

QUIOPNPA

API Открыть группу панелей для печати

QUHDSPH

API Показать справку

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKPNLGRP

Работа с группой панелей

Операции над уровнем готовности продукта (*PRDAVL)

В этом списке указаны операции, выполняемые над уровнем готовности продукта (*PRDAVL), и условия их контроля.

- Операция изменения

WRKSPTPRD

Работа с поддерживаемыми продуктами, если добавляется или удаляется поддержка продукта

- Операции, для которых контроль не включен

Чтение

Никакие операции чтения не контролируются

Операции над определением продукта (*PRDDFN)

В этом списке указаны операции, выполняемые над определением продукта (*PRDDFN), и условия их контроля.

- Операция изменения

ADDPRDLICI

Добавить информацию о лицензии на продукт

WRKSPTPRD

Работа с поддерживаемыми продуктами, если добавляется или удаляется поддержка продукта

- Операции, для которых контроль не включен

Чтение

Никакие операции чтения не контролируются

Операции над компоновкой программных продуктов (*PRDLOD)

В этом списке указаны операции, выполняемые над компоновкой программных продуктов (*PRDLOD), и условия их контроля.

- Операция изменения

Изменение

Состояние, список библиотек, список папок или основной язык компоновки программных продуктов

- Операции, для которых контроль не включен

Чтение

Никакие операции чтения не контролируются

Операции над формой Query Manager (*QMFORM)

В этом списке указаны операции, выполняемые над формой Query Manager (*QMFORM), и условия их контроля.

- Операция чтения

STRQMQR

Запустить запрос Управления запросами

RTVQMFORM

Получить форму Управления запросами

Запуск Выполнить запрос

Экспорт

Экспортировать форму Управления запросами

Печать

Печать формы Управления запросами

Печать отчета Управления запросами с помощью формы

Используйте

Обращение к форме с помощью опций 2, 5, 6 и 9 или функции F13 меню DB2 Query Manager и SQL Development Kit для i5/OS.

- Операция изменения

CRTQMFORM

Создать форму Управления запросами

IMPORT

Импортировать форму Управления запросами

Сохранить

Сохранить форму с помощью опции меню или команды

Копирование

Опция 3 меню Работа с формами Query Manager

- Операции, для которых контроль не включен

Работа с

Если в меню Работа с показаны объекты *QMFORM

Активен

Любая операция над активной формой.

Операции над запросом Query Manager (*QMQR)

В этом списке указаны операции, выполняемые над запросом Query Manager (*QMQR), и условия их контроля.

- Операция чтения

RTVQMQR

Получить запрос Query Manager

Запуск Выполнить запрос Query Manager

STRQMQR

Запустить запрос Query Manager

Экспорт

Экспортировать запрос Query Manager

Печать

Печать запроса Query Manager

Используйте

Обращение к запросу с помощью функции F13 или опции 2, 5, 6 или 9 меню Работа с запросами Query Manager

- Операция изменения

CRTQMQR

Создать запрос Управления запросами

Преобразование

Опция 10 (Преобразовать в SQL) меню Работа с запросами Query Manager

Копирование

Опция 3 меню Работа с запросами Query Manager

Сохранить

Сохранить запрос с помощью меню или команды

- Операции, для которых контроль не включен

Работа с

Если в меню Работа с показаны объекты *QMQRV

Активен

Любая операция над активным запросом.

Операции над определением запроса (*QRYDFN)

В этом списке указаны операции, выполняемые над определением запроса (*QRYDFN), и условия их контроля.

- Операция чтения

ANZQRY

Анализировать запрос

Изменение

Изменить запрос с помощью меню команды WRKQRY или QRY.

Просмотр

Показать запрос с помощью меню команды WRKQRY

Экспорт

Экспортировать форму с помощью Query Manager

Экспорт

Экспортировать запрос с помощью Query Manager

Печать

Печать определения запроса с помощью меню команды WRKQRY

Печать формы Управления запросами

Печать запроса Управления запросами

Печать отчета Управления запросами

QRYRUN

Выполнить запрос

RTVQMFORM

Получить форму Управления запросами

RTVQMQRV

Получить запрос Управления запросами

Запуск Выполнить запрос с помощью меню WRKQRY

Run (команда Управления запросами)

RUNQRY

Выполнить запрос

STRQMQRV

Запустить запрос Управления запросами

Передача на выполнение

Передать запрос на выполнение (запустить запрос) в пакетном режиме с помощью меню WRKQRY или меню Закончить работу с этим запросом

- Операция изменения

Изменение

Сохранить измененный запрос с помощью лицензионной программы Query/400

- Операции, для которых контроль не включен

Копирование

Скопировать запрос с помощью опции 3 меню “Работа с запросами”

Создание

Создать запрос с помощью опции 1 меню “Работа с запросами”

Удаление

Удалить запрос с помощью опции 4 меню “Работа с запросами”

Запуск Выполнить запрос путем выбора опции 1 меню “Закончить работу с этим запросом”, если запрос был создан или изменен с помощью лицензионной программы Query/400; выполнить запрос в интерактивном режиме с помощью PF5 при создании, просмотре или изменении запроса в лицензионной программе Query/400

DLTQRY

Удалить запрос

Операции над таблицей преобразования информационных кодов (*RCT)

В этом списке указаны операции, выполняемые над таблицей преобразования информационных кодов (*RCT), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

Нет

- Операции, для которых контроль не включен

Нет

Операции над списком ответов

В этом списке указаны операции, выполняемые над списком ответов, и условия их контроля.

Примечание: Действия над списком объектов контролируются в том случае, если в системном значении Контроль действий (QAUDLVL) или в параметре пользовательского профайла Контроль действий (AUDLVL) задано значение *SYSMGT.

- Операции, для которых включен контроль

ADDRPYLE

Добавить запись списка ответов

CHGRPYLE

Изменить запись списка ответов

RMVRPYLE

Удалить запись списка ответов

WRKRPYLE

Работа с записью списка ответов

- Операции, для которых контроль не включен

Нет

Операции над описанием подсистемы (*SBSD)

В этом списке указаны операции, выполняемые над описанием подсистемы (*SBSD), и условия их контроля.

- Операция чтения

ENDSBS

Завершить работу подсистемы

STRSBS

Запустить подсистему

- Операция изменения

ADDAJE

Добавить запись автоматического задания

ADDCMNE

Добавить запись средств связи

ADDJOBQE

Добавить запись очереди заданий

ADDPJE

Добавить запись предварительного задания

ADDRTGE

Добавить запись о выполнении

ADDWSE

Добавить запись рабочей станции

CHGAJE

Изменить запись автоматического задания

CHGCMNE

Изменить запись средств связи

CHGJOBQE

Изменить запись очереди заданий

CHGPJE

Изменить запись предварительного задания

CHGRTGE

Изменить запись о выполнении

CHGSBSD

Изменить описание подсистемы

CHGWSE

Изменить запись рабочей станции

RMVAJE

Удалить запись автоматического задания

RMVCMNE

Удалить запись средств связи

RMVJOBQE

Удалить запись очереди заданий

RMVPJE

Удалить запись предварительного задания

RMVRTGE

Удалить запись о выполнении

RMVWSE

Удалить запись рабочей станции

- Операции, для которых контроль не включен

DSPSBSD

Показать описание подсистемы

QWCLASBS

API Показать активную подсистему

QWDLJSBQ

API Показать очередь заданий подсистемы

QWDRSBSD

API Получить описание подсистемы

WRKSBSD

Работа с описанием подсистемы

WRKSBS

Работа с подсистемой

WRKSBSJOB

Работа с заданием подсистемы

Операции над индексом поиска информации (*SCHIDX)

В этом списке указаны операции, выполняемые над индексом поиска информации (*SCHIDX), и условия их контроля.

- Операция чтения

STRSCHIDX

Запустить индекс поиска

WRKSCHIDX

Работа с записью индекса поиска

- Операция изменения (контролируется, если параметр OBJAUD равен *CHANGE или *ALL)

ADDSCHIDX

Добавить запись индекса поиска

CHGSCHIDX

Изменить индекс поиска

RMVSCCHIDX

Удалить запись индекса поиска

- Операции, для которых контроль не включен

WRKSCHIDX

Работа с индексом поиска

Операции над локальным сокетом (*SOCKET)

В этом списке указаны операции, выполняемые над локальным сокетом (*SOCKET), и условия их контроля.

- Операция чтения

- connect**
Установить связывание между постоянным целевым расположением и сокетом и установить соединение.
- DSPLNK**
Показать ссылки
- givedescriptor**
API Предоставить доступ к файлу
- Qp01GetPathFromFileID**
API Получить полное имя объекта из ИД файла
- Qp01RenameKeep**
API Переименовать файл или каталог, сохранить новый экземпляр
- Qp01RenameUnlink**
API Переименовать файл или каталог, отключить новый экземпляр
- sendmsg**
Отправить дейтаграмму в режиме без установления соединения. Может применяться несколько буферов.
- sendto** Отправить дейтаграмму в режиме без установления соединения.
- WRKLNK**
Работа со ссылками
- Операция изменения
 - ADDLNK**
Добавить ссылку
 - bind** Установить локальный адрес сокета.
 - CHGAUD**
Изменить параметры контроля
 - CHGAUT**
Изменить права доступа
 - CHGOWN**
Изменить владельца
 - CHGPGP**
Изменить основную группу
 - CHKIN**
Вернуть
 - CHKOUT**
Изъять
 - chmod** API Изменить права доступа к файлу
 - chown** API Изменить владельца и группу
 - givedescriptor**
API Предоставить доступ к файлу
 - ссылка**
API Создать ссылку на файл
 - Qp01RenameKeep**
API Переименовать файл или каталог, сохранить новый экземпляр
 - Qp01RenameUnlink**
API Переименовать файл или каталог, отключить новый экземпляр

RMVLNK

Удалить ссылку

RNM Переименование

RST Восстановить

unlink API Удалить ссылку на файл

utime API Задать время изменения файла и обращения к нему

WRKAUT

Работа с правами доступа

WRKLNK

Работа со ссылками

- Операции, для которых контроль не включен

close API Закрыть файл

Примечание: Операция закрытия не контролируется, однако в случае возникновения сбоя или внесения изменения в программе выхода `scan_related` будет создана контрольная запись.

DSPAUT

Показать права доступа

dup API Скопировать дескриптор открытого файла

dup2 API Скопировать дескриптор открытого файла в другой дескриптор

fcntl API Выполнить команду управления файлами

fstat API Получить информацию о файле с помощью дескриптора

fsync API Синхронизировать изменения файла

ioctl API Выполнить запрос на управление вводом-выводом

lstat API Получить информацию о файле или связи

pathconf

API Получить настраиваемые переменные полного имени

чтение API Прочитать данные из файла

readv API Прочитать данные из файла (вектор)

select API Проверить состояние ввода-вывода нескольких дескрипторов файлов

stat API Получить информацию о файле

takedescriptor

API Принять права доступа к файлу

запись API Записать данные в файл

writev API Записать данные в файл (вектор)

Операции над орфографическим словарем (*SPADCT)

В этом списке указаны операции, выполняемые над орфографическим словарем (*SPADCT), и условия их контроля.

- Операция чтения

Проверка

Функция проверки орфографии

Помощь

Помощь в проверке орфографии

Перенос

Функция переноса

Отмена переноса

Функция отмена переноса

Синонимы

Функция подбора синонимов

Базовый

Применение словаря в качестве базового при создании другого словаря

Проверка

Применение словаря в качестве проверочного при создании другого словаря

Получение

Получить список общеупотребительных слов

Печать

Печать списка общеупотребительных слов

- Операция изменения

CRTSPADCT

Создать орфографический словарь с параметром REPLACE(*YES)

- Операции, для которых контроль не включен

Нет

Операции над буферными файлами

В этом списке указаны операции, выполняемые над буферными файлами, и условия их контроля.

Примечание: Действия над буферными файлами контролируются в том случае, если в системном значении Контроль действий (QAUDLVL) или в параметре пользовательского профайла Контроль действий (AUDLVL) задано значение *SPLFDTA.

- Операции, для которых включен контроль

Уровень прав доступа

Каждое обращение любого пользователя, кроме владельца буферного файла, в том числе:

- CPYSPLF
- DSPSPLF
- SNDNETSPLF
- SNDTCPSPLF
- STRRMTWTR
- API QSPONSP

Изменение

Изменение любого из следующих атрибутов буферного файла с помощью CHGSPLFA:

- COPIES
- DEV
- FORMTYPE
- RESTART
- PAGERANGE
- OUTQ

- DRAWER
- PAGDFN
- FORMDF
- USRDFNOPT
- USRDFNOBJ
- USRDFNDDTA
- EXPDATE
- SAVE

Изменение любых других атрибутов буферного файла с помощью CHGSPLFA:

Создание

Создание буферного файла с помощью операций печати

Создание буферного файла с помощью API QSPCRTSP

Удаление

Удаление буферного файла одним из следующих способов:

- Печать буферного файла с помощью загрузчика принтера или дискеты
- Очистка очереди вывода (CLROUTQ)
- Удаление буферного файла с помощью команды DLTSPLF или опции удаления, предусмотренной в меню работы с буферными файлами
- Удаление буферных файлов при завершении работы задания (ENDJOB SPLFILE(*YES))
- Удаление буферных файлов при завершении работы задания печати (ENDPJ SPLFILE(*YES))
- Отправка буферного файла в удаленную систему с помощью удаленного загрузчика
- Удаление устаревших буферных файлов с помощью команды DLTEXPSPLF
- Удаление буферных файлов с помощью функции очистки Операционной поддержки

Блокировка

Блокирование буферного файла одним из следующих способов:

- С помощью команды HLDSPLF
- С помощью опции блокирования, предусмотренной в меню работы с буферными файлами
- Печать буферного файла с параметром SAVE(*YES)
- Отправка буферного файла в удаленную систему с помощью удаленного загрузчика, если для буферного файла задан параметр SAVE(*YES)
- Блокирование буферного файла загрузчиком в случае возникновения ошибки при обработке буферного файла

Чтение

Чтение буферного файла загрузчиком принтера или дискеты

Разблокирование

Разблокирование буферного файла

Восстановить

Восстановление буферного файла

Сохранить

Сохранение буферного файла

Операции над пакетом SQL (*SQLPKG)

В этом списке указаны операции, выполняемые над пакетом SQL (*SQLPKG), и условия их контроля.

- Операция чтения

Запуск При выполнении объекта *SQLPKG

- Операция изменения

Нет

- Операции, для которых контроль не включен

PRTSQLINF

Печать информации SQL

Операции над служебной программой (*SRVPGM)

В этом списке указаны операции, выполняемые над служебной программой (*SRVPGM), и условия их контроля.

- Операция чтения

CRTPGM

Контрольная запись создается для каждой служебной программы, применяемой командой CRTPGM

CRTSRVPGM

Контрольная запись создается для каждой служебной программы, применяемой командой CRTSRVPGM

QTEDBGS

API Зарегистрировать представление отладки

QTEDBGS

API Получить представления модулей

RTVBNDSRC

Получить исходный файл редактора связей

UPDPGM

Контрольная запись создается для каждой служебной программы, применяемой командой UPDPGM.

UPDSRVPGM

Контрольная запись создается для каждой служебной программы, применяемой командой UPDSRVPGM.

- Операция создания

CRTSRVPGM

Создать служебную программу

UPDSRVPGM

Обновить служебную программу

- Операция изменения

CHGSRVPGM

Изменить служебную программу

- Операции, для которых контроль не включен

DSPSRVPGM

Показать служебную программу

PRTSQLINF

Печать информации SQL

QBNLSPGM

API Показать информацию о служебной программе

QBNRSPGM

API Получить информацию о служебной программе

WRKSRVPGM

Работа со служебной программой

Операции над описанием сеанса (*SSND)

В этом списке указаны операции, выполняемые над описанием сеанса (*SSND), и условия их контроля.

Никакие операции чтения и изменения объектов типа *SSND не контролируются.

Операции над областью памяти сервера (*SVRSTG)

В этом списке указаны операции, выполняемые над областью памяти сервера (*SVRSTG), и условия их контроля.

Никакие операции чтения и изменения объектов типа *SVRSTG не контролируются.

Операции над потоковым файлом (*STMF)

В этом списке указаны операции, выполняемые над потоковым файлом (*STMF), и условия их контроля.

- Операция чтения

CPY Скопировать объект

DSPLNK

Показать ссылки объекта

givedescriptor

API Предоставить доступ к файлу

MOV Переместить объект

open, open64, QlgOpen, QlgOpen64, Qp0IOpen

API Открыть файл

SAV Сохранить объекты

WRKLNK

Работа со ссылками объекта

- Операция изменения

ADDLNK

Добавить ссылку

CHGAUD

Изменить параметры контроля

CHGAUT

Изменить права доступа

CHGOWN

Изменить владельца

CHGPGP

Изменить основную группу

CHKIN

Вернуть объект

CHKOUT

Изъять объект

chmod, QlgChmod

API Изменить права доступа к файлу

- chown, QlgChown**
API Изменить владельца или группу
- CPY** Скопировать объект
- creat, creat64, QlgCreat, QlgCreat64**
API Создать файл или заменить файл
- fchmod**
API Изменить права доступа к файлу с помощью дескриптора
- fchown**
API Изменить владельца и группу файла с помощью дескриптора
- givedescriptor**
API Предоставить доступ к файлу
- ссылка**
API Создать ссылку на файл
- MOV** Переместить объект
- open, open64, QlgOpen, QlgOpen64, Qp0lOpen**
При открытии файла для записи с помощью API
- Qp0lGetPathFromFileID, QlgGetPathFromFileID**
API Получить полное имя объекта из ИД файла
- Qp0lRenameKeep, QlgRenameKeep**
API Переименовать файл или каталог, сохранить новый экземпляр
- Qp0lRenameUnlink, QlgRenameUnlink**
API Переименовать файл или каталог, отключить новый экземпляр
- RMVLNK**
Удалить ссылку
- RNM** Переименовать объект
- RST** Восстановить объект
- unlink, QlgUnlink**
API Удалить ссылку на файл
- utime, QlgUtime**
API Задать время изменения файла и обращения к нему
- WRKAUT**
Работа с правами доступа
- WRKLNK**
Работа со ссылками
- Операции, для которых контроль не включен
- close** API Закрыть файл
- DSPAUT**
Показать права доступа
- dup** API Скопировать дескриптор открытого файла
- dup2** API Скопировать дескриптор открытого файла в другой дескриптор
- faccessx**
Определить доступные файлы
- fclear, fclear64**
Очистить файл

fcntl API Выполнить команду управления файлами

fpathconf
API Получить настраиваемые переменные полного имени с помощью дескриптора

fstat, fstat64
API Получить информацию о файле с помощью дескриптора

fsync API Синхронизировать изменения файла

ftruncate, ftruncate64
API Усечь файл

ioctl API Выполнить запрос на управление вводом-выводом

lseek, lseek64
API Задать смещение в файле для чтения/записи

lstat, lstat64
API Получить информацию о файле или связи

pathconf, QlgPathconf
API Получить настраиваемые переменные полного имени

pread, pread64
API Прочитать данные с заданным смещением из дескриптора

pwrite, pwrite64
API Записать данные с заданным смещением в дескриптор

чтение API Прочитать данные из файла

readv API Прочитать данные из файла (вектор)

select API Проверить состояние ввода-вывода нескольких дескрипторов файлов

stat, stat64, QlgStat, QlgStat64
API Получить информацию о файле

takedescriptor
API Принять права доступа к файлу

запись API Записать данные в файл

writev API Записать данные в файл (вектор)

Операции над символическими ссылками (*SYMLNK)

В этом списке указаны операции, выполняемые над символическими ссылками (*SYMLNK), и условия их контроля.

- Операция чтения

CPY Скопировать объект

DSPLNK

Показать ссылки объекта

MOV Переместить объект

readlink

API Прочитать значение символической связи

SAV Сохранить объекты

WRKLNK

Работа со ссылками объекта

- Операция изменения

CHGOWN

Изменить владельца

CHGPGP

Изменить основную группу

CPY Скопировать объект

MOV Переместить объект

Qp0IRenameKeep, QlgRenameKeep

API Переименовать файл или каталог, сохранить новый экземпляр

Qp0IRenameUnlink, QlgRenameUnlink

API Переименовать файл или каталог, отключить новый экземпляр

RMVLNK

Удалить ссылку

RNM Переименовать объект

RST Восстановить объект

symlink, QlgSymlink

API Установить символическую ссылку

unlink, QlgUnlink

API Удалить ссылку на файл

WRKLNK

Работа со ссылками объекта

- Операции, для которых контроль не включен

Istat, Istat64, QlgIstat, QlgIstat64

API Состояние связи

Операции над описанием системы S/36 (*S36)

В этом списке указаны операции, выполняемые над описанием системы S/36 (*S36), и условия их контроля.

- Операция чтения

Нет

- Операция изменения

CHGS36

Изменить конфигурацию S/36

CHGS36A

Изменить атрибуты конфигурации S/36

SET Процедура SET

CRTDEVXXX

При добавлении устройства в таблицу конфигурации

DLTDEV

При удалении устройства из таблицы конфигурации

RNMOBJ

Переименовать описание устройства

- Операции, для которых контроль не включен

DSPS36

Показать конфигурацию S/36

RTVS36A

Получить атрибуты конфигурации S/36

STRS36

Запустить S/36

ENDS36

Завершить работу S/36

Операции над таблицей (*TBL)

В этом списке указаны операции, выполняемые над таблицей (*TBL), и условия их контроля.

- Операция чтения

QDCXLATE

Преобразовать строку символов

QTBXLATE

Преобразовать строку символов

QLGRTVSS

Получить таблицу последовательности сортировки

CRTL F

Применение таблицы преобразования при выполнении команды CTRL F

Чтение

Применение таблицы последовательности сортировки при выполнении любой команды, в которой задана последовательность сортировки

- Операция изменения

Нет

- Операции, для которых контроль не включен

WRKTBL

Работа с таблицей

Операции над пользовательским индексом (*USRIDX)

В этом списке указаны операции, выполняемые над пользовательским индексом (*USRIDX), и условия их контроля.

- Операция чтения

QUSRTVUI

API Получить записи пользовательского индекса

- Операция изменения

QUSADDUI

API Добавить записи пользовательского индекса

QUSRMVUI

API Удалить записи пользовательского индекса

- Операции, для которых контроль не включен

Уровень прав доступа

Прямое обращение к пользовательскому индексу с помощью команд машинного интерфейса (допустимо только для пользовательского индекса из пользовательского домена, расположенного в библиотеке, указанной в системном значении QALWUSRDMN).

QUSRUIAT

API Получить атрибуты пользовательского индекса

Операции над пользовательским профайлом (*USRPRF)

В этом списке указаны операции, выполняемые над пользовательским профайлом (*USRPRF), и условия их контроля.

- Операция чтения

RCLOBJOWN

Восстановить объекты по владельцу

- Операция изменения

CHGPRF

Изменить профайл

CHGPWD

Смена пароля

CHGUSRPRF

Изменить пользовательский профайл

CHKPWD

Проверить пароль

DLTUSRPRF

Удалить пользовательский профайл

GRTUSRAUT

Предоставить права доступа пользователю (*целевой-пользовательский-профайл*)

QSYCHGPW

API Изменить пароль

RSTUSRPRF

Восстановить пользовательский профайл

- Операции, для которых контроль не включен

DSPPGMADP

Показать принимающие программы

DSPUSRPRF

Показать пользовательский профайл

GRTUSRAUT

Предоставить права доступа пользователю (*исходный-пользовательский-профайл*)

PRTPRFINT

Печать внутренних данных профайла

PRTUSRPRF

Печать пользовательского профайла

QSYCUSRS

API Проверить специальные права доступа пользователя

QSYLOBJA

API Показать доступные объекты

QSYLOBJP

API Показать объекты, принимающие права доступа

QSYRUSRI

API Получить информацию о пользователе

RTVUSRPRF

Получить пользовательский профайл

WRKOBJOWN

Работа с принадлежащими пользователю объектами

WRKUSRPRF

Работа с пользовательскими профайлами

Операции над пользовательской очередью (*USRQ)

В этом списке указаны операции, выполняемые над пользовательской очередью (*USRQ), и условия их контроля.

- Никакие операции чтения и изменения объектов типа *USRQ не контролируются.
- Операции, для которых контроль не включен

Уровень прав доступа

Прямое обращение к пользовательской очереди с помощью команд машинного интерфейса (допустимо только для пользовательской очереди из пользовательского домена, расположенной в библиотеке, указанной в системном значении QALWUSRDMN).

Операции над пользовательским пространством (*USRSPC)

В этом списке указаны операции, выполняемые над пользовательским пространством (*USRSPC), и условия их контроля.

- Операция чтения

QUSRTVUS

API Получить пользовательское пространство

- Операция изменения

QUSCHGUS

API Изменить пользовательское пространство

QUSCUSAT

API Изменить атрибуты пользовательского пространства

- Операции, для которых контроль не включен

Уровень прав доступа

Прямое обращение к пользовательскому пространству с помощью команд машинного интерфейса (допустимо только для пользовательского пространства из пользовательского домена, расположенного в библиотеке, указанной в системном значении QALWUSRDMN).

QUSRUSAT

API Получить атрибуты пользовательского пространства

Операции над контрольным списком (*VLDL)

В этом списке указаны операции, выполняемые над контрольным списком (*VLDL), и условия их контроля.

- Операция чтения

QSYFDVLE

API Найти запись контрольного списка

- Операция изменения

QSYADVLE

API Добавить запись контрольного списка

QSYCHVLE

API Изменить запись контрольного списка

QSYRMVLE

API Удалить запись контрольного списка

Операции над объектом настройки рабочей станции (*WSCST)

В этом списке указаны операции, выполняемые над объектом настройки рабочей станции (*WSCST), и условия их контроля.

- Операция чтения

Изменение состояния

Если настроенное устройство включено

RTVWSCST

Получить исходный текст объекта настройки рабочей станции (если тип устройства равен *TRANSFORM)

SNDDTCPSPLF

Отправить буферный файл по TCP/IP (если указано TRANSFORM(*YES))

STRPRTWTR

Запустить загрузчик принтера (только при печати буферного файла на настроенном принтере с помощью функции преобразования печати хоста)

STRRMWTR

Запустить удаленный загрузчик (если для очереди вывода заданы параметры CNNTYPE(*IP) и TRANSFORM(*YES))

Печать

При печати вывода без буферизации на настроенном принтере с помощью функции преобразования печати хоста

- Операция изменения

Нет

- Операции, для которых контроль не включен

Нет

Приложение F. Макет записей журнала контроля

В этом разделе содержится информация о форматах всех типов записей журнала контроля (QAUDJRN) с кодом T. Для управления этими записями служат значения контроля действий и объектов, определяемые пользователем.

| Макеты записей журнала, описанные в этом разделе, аналогичны определению физических файлов с помощью DDS. Например, тип Binary (4) предназначен для хранения от 1 до 4 цифр и резервирует 2 байта памяти, а тип Binary (5) предназначен для хранения от 1 до 5 цифр и резервирует 4 байта памяти. Такие языки как RPG применяют эти определения. Система заносит в журнал контроля дополнительные записи о таких событиях, как IPL системы или сохранение получателя журнала. Форматы записей этих типов описаны в разделе Управление журналами.

В “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597 описан формат полей, которые являются общими для всех записей в случае, если при запуске команды DSPJRN был указан параметр OUTFILFMT(*TYPE2). Определение данного формата, который называется QJORDJE2, содержится в файле QADSPJR2 из библиотеки QSYS.

В “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 описан формат полей, которые являются общими для записей всех типов в случае, если при запуске команды DSPJRN был указан параметр OUTFILFMT(*TYPE4). Определение данного формата, который называется QJORDJE4, содержится в файле QADSPJR4 из библиотеки QSYS. Формат вывода *TYPE4 включает все данные формата *TYPE2, а также сведения о получателях журналов, триггерах и ограничениях по ссылкам.

Примечание: Выпуск обновлений для форматов вывода *TYPE2 и *TYPE4 прекращен. В связи с этим рекомендуется отказаться от применения форматов *TYPE2 и *TYPE4 и использовать только форматы *TYPE5.

В “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 описан формат полей, которые являются общими для записей всех типов, если при запуске команды DSPJRN был указан параметр OUTFILFMT(*TYPE5). Определение данного формата, который называется QJORDJE5, содержится в файле QADSPJR5 из библиотеки QSYS. Формат вывода *TYPE5 включает все данные формата *TYPE4, а также сведения о библиотеке программы, имя ASP программы, номер ASP программы, имя получателя, библиотеку получателя, имя ASP получателя, номер ASP получателя, номер диска, ИД нити, семейство адресов, удаленный порт и удаленный адрес.

В “Записи журнала AD (изменение параметров контроля)” на стр. 600 - “Записи журнала ZR (чтение объекта)” на стр. 743 описаны форматы файлов вывода модельной базы данных, позволяющие определить содержательную часть записи. С помощью команды CRTDUPOBJ можно создать пустой файл вывода, формат которого будет совпадать с форматом одного из файлов вывода модельной базы данных. Команда DSPJRN позволяет скопировать выбранные записи журнала контроля в файл вывода для последующего анализа. В разделе “Анализ записей журнала контроля с помощью утилиты запроса или программы” на стр. 315 приведены примеры применения файлов вывода модельной базы данных. Дополнительную информацию можно найти в разделе Управление журналами.

| **Примечание:** В этих таблицах записей журнала встречаются пустые столбцы Смещение, JE или J4. Это означает, что для этого типа журнала нет модельного файла вывода.

Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)

В этой таблице описаны возможные значения полей, которые являются общими для всех записей в случае, если при вызове команды DSPJRN был указан параметр OUTFILFMT(*TYPE5).

Таблица 156. Стандартные поля заголовков для записей журнала контроля. Формат записи QJORDJE5 (*TYPE5)

Смещ.	Поле	Отформатированно	Описание
1	Длина записи	Zoned(5,0)	Общая длина записи журнала с учетом поля длины записи.
6	Порядковый номер	Char(20)	Присваивается всем записям журнала. Начальное значение для каждого нового или восстановленного журнала - 1. Данному параметру можно присвоить значение 1 при подключении нового получателя.
26	Код журнала	Char(1)	Всегда равен T.
27	Тип записи	Char(2)	Список типов записей и их описание приведены в разделе “Типы записей журнала контроля (QAUDJRN)” на стр. 598.
29	Системное время записи	Char(26)	Дата и время создания записи в формате SAA.
55	Имя задания	Char(10)	Имя задания, послужившего причиной создания записи.
65	Имя польз.	Char(10)	Имя пользовательского профайла, связанного с заданием ¹ .
75	Номер задания	Zoned(6,0)	Номер задания.
81	Имя программы	Char(10)	Имя программы, создавшей запись журнала. Это может быть как имя служебной программы, так и неполное имя файла класса, применяемого в откомпилированной программе на Java. Если запись была создана не прикладной программой и не программой на CL, это поле содержит имя системной программы, такой как QCMD. Данное поле содержит значение *NONE в следующих случаях: <ul style="list-style-type: none"> Имя программы не указывается в записях этого типа. Имя программы неизвестно.
91	Библиотека программы	Char(10)	Имя библиотеки, которая содержит программу, создавшую запись журнала.
101	ASP программы	Char(10)	Имя ASP, содержащего программу, создавшую запись журнала.
111	Номер ASP программы	Zoned(5,0)	Номер ASP, содержащего программу, создавшую запись журнала.
116	Имя объекта	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
126	Библиотека объектов	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
136	Имя элемента	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
146	Число/RRN	Char(20)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
166	Флаг	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
167	ИД цикла фиксации	Char(20)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
187	Пользовательский профайл	Char(10)	Имя текущего пользовательского профайла ¹ .
197	Имя системы	Char(8)	Имя системы.

Таблица 156. Стандартные поля заголовков для записей журнала контроля (продолжение). Формат записи QJORDJE5 (*TYPE5)

Смещ.	Поле	Отформатировано	Описание
205	ИД журнала	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
215	Ограничение по ссылкам	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
216	Триггер	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
217	Неполные данные	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
218	Игнорирование в APY/ RMVJRNCHG	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
219	Минимальный ESD	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
220	Индикатор объекта	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
221	Порядковый номер в системе	Char(20)	Число, присваиваемое системой каждой записи журнала.
241	Получатель	Char(10)	Имя получателя, содержащего запись журнала.
251	Библиотека получателя	Char(10)	Имя библиотеки получателя, содержащего запись журнала.
261	ASP получателя	Char(10)	Имя ASP, содержащего получателя.
271	Номер ASP получателя	Zoned(5,0)	Номер ASP, в котором расположен получатель, содержащий запись журнала.
276	Номер дискового накопителя	Zoned(5,0)	Номер дискового накопителя, на котором расположена запись журнала.
281	ИД нити	Hex(8)	Идентификатор нити процесса, создавшей запись журнала.
289	Шест. ИД нити	Char(16)	Отображаемый идентификатор нити в шестнадцатеричном формате.
305	Семейство адресов	Char(1)	Формат удаленного адреса данной записи журнала.
306	Удаленный порт	Zoned(5,0)	Номер порта удаленного адреса, связанного с данной записью журнала.
311	Удаленный адрес	Char(46)	Удаленный адрес, связанный с данной записью журнала.
357	Логическая единица работы	Char(39)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
396	ИД транзакции	Char(140)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
536	Зарезерв.	Char(20)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
556	Индикатор пустого значения	Char(50)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
606	Длина содержательной части записи	Binary(5)	Длина данных, содержащихся в записи.

Таблица 156. Стандартные поля заголовков для записей журнала контроля (продолжение). Формат записи QJORDJE5 (*TYPE5)

Смещ.	Поле	Отформатиров.	Описание
<p>Примечание: Имя системного задания состоит из содержимого трех последовательных полей, первое из которых имеет смещение 55. В большинстве случаев поле Имя пользователя со смещением 65 и поле Имя пользовательского профайла со смещением 187 совпадают. Для предварительных заданий поле Имя пользовательского профайла содержит имя пользователя, запустившего транзакцию. Для некоторых заданий оба поля содержат имя пользователя QSYS. В содержательной части записи поле Имя пользовательского профайла содержит имя пользователя, создавшего запись. Если пользовательский профайл был заменен с помощью API, то в поле Имя пользовательского профайла будет указано имя нового (замещающего) пользовательского профайла.</p>			

Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)

В этой таблице описаны возможные значения полей, которые являются общими для всех записей в случае, если при вызове команды DSPJRN был указан параметр OUTFILFMT(*TYPE4).

Таблица 157. Стандартные поля заголовков для записей журнала контроля. Формат записи QJORDJE4 (*TYPE4)

Смещ.	Поле	Отформатиров.	Описание
1	Длина записи	Zoned(5,0)	Общая длина записи журнала с учетом поля длины записи.
6	Порядковый номер	Zoned(10,0)	Присваивается всем записям журнала. Начальное значение для каждого нового или восстановленного журнала - 1. Данному параметру можно присвоить значение 1 при подключении нового получателя.
16	Код журнала	Char(1)	Всегда равен T.
17	Тип записи	Char(2)	Список типов записей и их описание приведены в разделе “Типы записей журнала контроля (QAUDJRN)” на стр. 598.
19	Системное время записи	Char(26)	Дата и время создания записи в формате SAA.
45	Имя задания	Char(10)	Имя задания, послужившего причиной создания записи.
55	Имя польз.	Char(10)	Имя пользовательского профайла, связанного с заданием ¹ .
65	Номер задания	Zoned(6,0)	Номер задания.
71	Имя программы	Char(10)	Имя программы, создавшей запись журнала. Это может быть как имя служебной программы, так и неполное имя файла класса, применяемого в откомпилированной программе на Java. Если запись была создана не прикладной программой и не программой на CL, это поле содержит имя системной программы, такой как QCMD. Данное поле содержит значение *NONE в следующих случаях: <ul style="list-style-type: none"> Имя программы не указывается в записях этого типа. Имя программы неизвестно.
81	Имя объекта	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
91	Имя библиотеки	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
101	Имя элемента	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
111	Число/RRN	Zoned(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
121	Флаг	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.

Таблица 157. Стандартные поля заголовков для записей журнала контроля (продолжение). Формат записи QJORDJE4 (*TYPE4)

Смещ.	Поле	Отформатировано	Описание
122	ИД цикла фиксации	Zoned(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
132	Пользовательский профайл	Char(10)	Имя текущего пользовательского профайла ¹ .
142	Имя системы	Char(8)	Имя системы.
150	Идентификатор журнала	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
160	Ограничение по ссылкам	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
161	Триггер	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
162	(Зарезерв.)	Char(8)	
170	Индикаторы пустого значения	Char(50)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
220	Длина содержательной части записи	Binary (4)	Длина данных, содержащихся в записи.
<p>Примечание: Имя системного задания состоит из содержимого трех последовательных полей, первое из которых имеет смещение 45. В большинстве случаев поле Имя пользователя со смещением 55 и поле Имя пользовательского профайла со смещением 132 совпадают. Для предварительных заданий поле Имя пользовательского профайла содержит имя пользователя, запустившего транзакцию. Для некоторых заданий оба поля содержат имя пользователя QSYS. В содержательной части записи поле Имя пользовательского профайла содержит имя пользователя, создавшего запись. Если пользовательский профайл был заменен с помощью API, то в поле Имя пользовательского профайла будет указано имя нового (замещающего) пользовательского профайла.</p>			

Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)

В этой таблице описаны возможные значения полей, которые являются общими для всех записей в случае, если при вызове команды DSPJRN был указан параметр OUTFILFMT(*TYPE2).

Таблица 158. Стандартные поля заголовков для записей журнала контроля. Формат записи QJORDJE2 (*TYPE2)

Смещ.	Поле	Отформатировано	Описание
1	Длина записи	Zoned(5,0)	Общая длина записи журнала с учетом поля длины записи.
6	Порядковый номер	Zoned(10,0)	Присваивается всем записям журнала. Начальное значение для каждого нового или восстановленного журнала - 1. Данному параметру можно присвоить значение 1 при подключении нового получателя.
16	Код журнала	Char(1)	Всегда равен T.
17	Тип записи	Char(2)	Список типов записей и их описание приведены в разделе “Типы записей журнала контроля (QAUDJRN)” на стр. 598.
19	Системное время	Char(6)	Системная дата на момент создания записи.
25	Системное время записи	Zoned(6,0)	Значение системного времени на момент создания записи.
31	Имя задания	Char(10)	Имя задания, послужившего причиной создания записи.

Таблица 158. Стандартные поля заголовков для записей журнала контроля (продолжение). Формат записи QJORDJE2 (*TYPE2)

Смещ.	Поле	Отформатировано	Описание
41	Имя польз.	Char(10)	Имя пользовательского профайла, связанного с заданием ¹ .
51	Номер задания	Zoned(6,0)	Номер задания.
57	Имя программы	Char(10)	Имя программы, создавшей запись журнала. Это может быть как имя служебной программы, так и неполное имя файла класса, применяемого в откомпилированной программе на Java. Если запись была создана не прикладной программой и не программой на CL, это поле содержит имя системной программы, такой как QCMD. Данное поле содержит значение *NONE в следующих случаях: <ul style="list-style-type: none"> Имя программы не указывается в записях этого типа. Имя программы неизвестно.
67	Имя объекта	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
77	Имя библиотеки	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
87	Имя элемента	Char(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
97	Число/RRN	Zoned(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
107	Флаг	Char(1)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
108	ИД цикла фиксации	Zoned(10)	Задается для объектов с журналами. Не указывается в записях журнала контроля.
118	Пользовательский профайл	Char(10)	Имя текущего пользовательского профайла ¹ .
128	Имя системы	Char(8)	Имя системы.
136	(Зарезерв.)	Char(20)	
<p>¹ Имя системного задания состоит из содержимого трех последовательных полей, первое из которых имеет смещение 31. В большинстве случаев поля <i>Имя пользователя</i> со смещением 41 и <i>Имя пользовательского профайла</i> со смещением 118 совпадают. Для предварительных заданий поле <i>Имя пользовательского профайла</i> содержит имя пользователя, запустившего транзакцию. Для некоторых заданий оба поля содержат имя пользователя QSYS. В содержательной части записи поле <i>Имя пользовательского профайла</i> содержит имя пользователя, создавшего эту запись. Если пользовательский профайл был заменен с помощью API, то в поле <i>Имя пользовательского профайла</i> будет указано имя нового (замещающего) пользовательского профайла.</p>			

Типы записей журнала контроля (QAUDJRN)

В этой таблице представлены все типы записей журнала контроля.

Таблица 159. Типы записей журнала контроля (QAUDJRN)

Тип записи	Описание
AD	Изменение параметров контроля
AF	Отсутствие необходимых прав доступа
AP	Принятие прав доступа
AU	Изменение атрибутов
CA	Изменение прав доступа
CD	Контроль командной строки

Таблица 159. Типы записей журнала контроля (QAUDJRN) (продолжение)

Тип записи	Описание
CO	Создание объекта
CP	Изменение, создание или восстановление пользовательского профайла
CQ	Изменение объекта *CRQD
CU	Операции с кластерами
CV	Проверка соединения
CY	Настройка шифрования
DI	Сервер каталогов
DO	Удаление объекта
DS	Сброс пароля защиты DST
EV	Переменные среды системы
GR	Шаблон записи
GS	Передача описания сокета другому заданию
IM	Монитор вторжений
IP	Обмен данными между процессами
IR	Действия правил IP
IS	Управление защитой в Internet
JD	Изменение параметра пользователя в описании задания
JS	Действия, влияющие на выполнение заданий
KF	Файл набора ключей
LD	Подключение, отключение или поиск записи каталога
ML	Действия с почтой служб Office
NA	Изменение сетевого атрибута
ND	Нарушение фильтра поиска в каталоге APPN
NE	Нарушение фильтра конечной точки APPN
OM	Перемещение или переименование объекта
OR	Восстановление объекта
OW	Изменение принадлежности объекта
O1	(Доступ к оптической памяти) Одиночный файл или каталог
O2	(Доступ к оптической памяти) Парный файл или каталог
O3	(Доступ к оптической памяти) Том
PA	Изменение программы для принятия прав доступа
PG	Изменение основной группы объекта
PO	Вывод на принтер
PS	Замена профайла
PW	Неверный пароль
RA	Изменение прав доступа при восстановлении
RJ	Восстановление описания задания с данными о пользовательском профайле
RO	Изменение владельца объекта при восстановлении
RP	Восстановление программы, принимающей права доступа
RQ	Восстановление объекта *CRQD

Таблица 159. Типы записей журнала контроля (QAUDJRN) (продолжение)

Тип записи	Описание
RU	Восстановление прав доступа пользовательского профайла
RZ	Изменение основной группы при восстановлении
SD	Изменение системного каталога рассылки
SE	Изменение записи о выполнении подсистемы
SF	Действия с буферными файлами
SG	Асинхронные сигналы
SK	Соединения SSL
SM	Изменение параметров управления системами
SO	Действия с пользовательской информацией о защите сервера
ST	Применение сервисных средств
SV	Изменение системного значения
VA	Изменение списка управления доступом
VC	Запуск или завершение соединения
VF	Закрытие файлов сервера
VL	Превышение ограничения учетной записи
VN	Вход и выход из сети
VO	Действия с контрольным списком
VP	Неверный сетевой пароль
VR	Обращение к сетевым ресурсам
VS	Запуск или завершение сеанса работы с сервером
VU	Изменение сетевого профайла
VV	Изменение состояния службы
X0	Идентификация в сети
X1	Маркер идентификации
XD	Расширение сервера каталогов
YC	Обращение к объекту DLO (изменение)
YR	Обращение к объекту DLO (чтение)
ZC	Обращение к объекту (изменение)
ZR	Обращение к объекту (чтение)

Записи журнала AD (изменение параметров контроля)

В этой таблице представлен формат записей журнала AD (изменение параметров контроля)

Таблица 160. Записи журнала AD (изменение параметров контроля). Файл описания полей QASYADJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	<p>D Команда CHGDLOAUD</p> <p>O Команда CHGOBJAUD или CHGAUD</p> <p>S Атрибут просмотра был изменен с помощью команды CHGATR или API Qp0!SetAttr, либо при создании объекта.</p> <p>U Команда CHGUSRAUD</p>
157	225	611	Имя объекта	Char(10)	Имя объекта, для которого были изменены параметры контроля.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки объекта.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Значение контроля для объекта	Char(10)	Для записей типов D, O и U поле содержит заданное значение контроля. Для записи типа S поле содержит значение атрибута просмотра.
195	263	649	CHGUSRAUD *CMD	Char(1)	Y = Команды контроля для данного пользователя.
196	264	650	CHGUSRAUD *CREATE	Char(1)	Y = Создавать запись контроля при создании объекта данным пользователем.
197	265	651	CHGUSRAUD *DELETE	Char(1)	Y = Создавать запись контроля при удалении объекта данным пользователем.
198	266	652	CHGUSRAUD *JOBDA	Char(1)	Y = Создавать запись контроля при изменении задания данным пользователем.
199	267	653	CHGUSRAUD *OBJMGT	Char(1)	Y = Создавать запись контроля при перемещении или переименовании объекта данным пользователем.
200	268	654	CHGUSRAUD *OFCSRV	Char(1)	Y = Создавать запись контроля при использовании данным пользователем функций Office.
201	269	655	CHGUSRAUD *PGMADP	Char(1)	Y = Создавать запись контроля при получении данным пользователем прав доступа с помощью принятых прав доступа.
202	270	656	CHGUSRAUD *SAVRST	Char(1)	Y = Создавать запись контроля при сохранении и восстановлении объектов данным пользователем.
203	271	657	CHGUSRAUD *SECURITY	Char(1)	Y = Создавать запись контроля при выполнении данным пользователем действий, связанных с защитой системы.

Таблица 160. Записи журнала AD (изменение параметров контроля) (продолжение). Файл описания полей QASYADJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
204	272	658	CHGUSRAUD *SERVICE	Char(1)	Y = Создавать запись контроля при запуске данным пользователем служебных функций.
205	273	659	CHGUSRAUD *SPLFDTA	Char(1)	Y = Создавать запись контроля при работе данного пользователя с буферными файлами.
206	274	660	CHGUSRAUD *SYSMGT	Char(1)	Y = Создавать запись контроля при изменении параметров управления системами данным пользователем.
207	275	661	CHGUSRAUD *OPTICAL	Char(1)	Y = Создавать запись контроля при обращении данного пользователя к оптическим накопителям.
208	276	662	CHGUSRAUD *AUTFAIL	Char(1)	Y = Создавать запись контроля при ошибке авторизации пользователя.
		663	CHGUSRAUD *JOBBAS	Char(1)	Y = Создавать запись контроля при выполнении функции работы с заданием пользователем.
		664	CHGUSRAUD *JOBCHGUSR	Char(1)	Y = Создавать запись контроля, когда пользователь изменяет активный профайл пользователя нити или файл группы.
		665	CHGUSRAUD *NETBAS	Char(1)	Y = Создавать запись контроля при выполнении функции работы с сетью пользователем.
		666	CHGUSRAUD *NETCLU	Char(1)	Y = Создавать запись контроля, когда пользователь вызывает функцию работы с кластером или группой ресурсов кластера.
		667	CHGUSRAUD *NETCMN	Char(1)	Y = Создавать запись контроля при выполнении функции связи в сети пользователем.
		668	CHGUSRAUD *NETFAIL	Char(1)	Y = Создавать запись контроля при ошибке сети для пользователя.
		669	CHGUSRAUD *NETSCK	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет задачи с сокетом.
		670	CHGUSRAUD *PGMFAIL	Char(1)	Y = Создавать запись контроля при ошибке программы для пользователя.
		671	CHGUSRAUD *PRTDTA	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет задачи печати с параметром SPOOL(*NO).
		672	CHGUSRAUD *SECCFG	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет задачи настройки защиты.
		673	CHGUSRAUD *SECDIRSRV	Char(1)	Y = Создавать запись контроля, когда пользователь вносит изменения или обновления с помощью функций службы каталогов.
		674	CHGUSRAUD *SECIPC	Char(1)	Y = Создавать запись контроля, когда пользователь изменяет взаимодействие между процессами.
		675	CHGUSRAUD *SECNAS	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет действия, связанные с службами сетевой идентификации.
		676	CHGUSRAUD *SECRUN	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет действия, связанные с средой защиты.

Таблица 160. Записи журнала AD (изменение параметров контроля) (продолжение). Файл описания полей QASYADJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		677	CHGUSRAUD *SECSCKD	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет действия, связанные с дескрипторами сокетов.
		678	CHGUSRAUD *SECVFY	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет действия, связанные с проверкой.
		679	CHGUSRAUD *SECVLDL	Char(1)	Y = Создавать запись контроля, когда пользователь выполняет действия с контрольными списками.
		680	(Зарезерв.)	Char(19)	
227	295	681	Имя DLO	Char(12)	Имя объекта DLO, для которого были изменены параметры контроля.
239	307	693	(Зарезерв.)	Char(8)	
247	315	701	Полное имя папки	Char(63)	Полное имя папки.
310			(Зарезерв.)	Char(20)	
	378	764	(Зарезерв.)	Char(18)	
	396	782	Длина имени объекта ¹	Binary(4)	Длина имени объекта.
330	398	784	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
334	402	788	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
336	404	790	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
339	407	793	(Зарезерв.)	Char(3)	
342	410	796	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
358	426	812	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
374	442	828	Имя объекта ¹	Char(512)	Имя объекта.
	954	1340	ИД файла объекта ¹	Char(16)	ИД файла объекта.
	970	1356	Имя ASP ⁵	Char(10)	Имя ASP.
	980	1366	Номер ASP ⁵	Char(5)	Номер ASP.
	985	1371	CCSID имени пути ¹	Binary(5)	Идентификатор набора символов, связанный с путем.
	989	1375	ИД страны или региона для полного пути ¹	Char(2)	ИД страны или региона, связанный с именем пути.
	991	1377	ИД языка для полного пути ¹	Char(3)	ИД языка, связанный с именем пути.

Таблица 160. Записи журнала AD (изменение параметров контроля) (продолжение). Файл описания полей QASYADJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	994	1380	Длина имени пути ¹	Binary(4)	Длина имени пути.
	996	1382	Индикатор пути ¹	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	997	1383	Отн. ИД каталога ^{1,3}	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1013	1399	Путь ^{1,4}	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁵ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала AF (ошибка прав доступа)

В этой таблице представлен формат записей журнала AF (ошибка прав доступа)

Таблица 161. Записи журнала AF (ошибка прав доступа). Файл описания полей QASYAFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.

Таблица 161. Записи журнала AF (ошибка прав доступа) (продолжение). Файл описания полей QASYAFJE/J4/J5

Смещ.			Поле	Отформатиро	Описание
JE	J4	J5			
156	224	610	Тип нарушения ¹	Char(1)	<p>A Нет прав доступа к объекту</p> <p>B Запрещенная команда</p> <p>C Не пройдена проверка (см. J5, смещение 639)</p> <p>D Применение неподдерживаемого интерфейса, ошибка домена объекта</p> <p>E Ошибка аппаратной защиты памяти, выход за границы постоянной памяти программы</p> <p>F Ошибка при проверке прав доступа ICAP</p> <p>G Ошибка идентификации ICAP</p> <p>H Действие программы выхода из процедуры просмотра (см. J5, смещение 639)</p> <p>I⁷ Запрещено наследование Java для системы</p> <p>J Ошибка профайла, передавшего задание на выполнение</p> <p>K Специальные права доступа</p> <p>Нет Кратковременное разрешение не является восстанавливаемым</p> <p>O Нет необходимых прав доступа к объекту оптической памяти</p> <p>P Ошибка замены профайла</p> <p>Ч Ошибка аппаратной защиты</p> <p>S Попытка входа в систему по умолчанию</p> <p>T Нет прав доступа к порту TCP/IP</p> <p>U Запрошены недопустимые права доступа пользователя</p> <p>V Кратковременное разрешение не позволяет создать новое разрешение</p> <p>W Кратковременное разрешение не позволяет выполнить замену профайлов</p> <p>X Системное нарушение — коды нарушений приведены в описании J5, смещение 723</p> <p>Д Нет прав доступа к текущему полю JUID при очистке JUID.</p> <p>Z Нет прав доступа к текущему полю JUID при настройке JUID.</p>
157	225	611	Имя объекта ^{1, 5, 12, 17}	Char(10)	Имя объекта.

Таблица 161. Записи журнала AF (ошибка прав доступа) (продолжение). Файл описания полей QASYAFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
167	235	621	Имя библиотеки ¹³	Char(10)	Имя библиотеки, в которой расположен объект, либо номер исправления Лицензионного внутреннего кода, которое не удалось применить. ¹¹
177	245	631	Тип объекта ^{14, 17}	Char(8)	Тип объекта.

Таблица 161. Записи журнала AF (ошибка прав доступа) (продолжение). Файл описания полей QASYAFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JЕ	J4	J5			
185	253	639	Действие при ошибке проверки	Char(1)	<p>Действие, которое выполняется при возникновении ошибки проверки; задается только в том случае, если тип нарушения (J5, смещение 610) равен С или Н.</p> <p>А Преобразование объекта не выполнялось или не было успешно завершено. Системное значение QALWOBJRST допускает восстановление объекта. пользователя не было специальных прав доступа *ALLOBJ, и уровень защиты системы был равен 10, 20 или 30. Все права доступа к объекту были сохранены.</p> <p>В Преобразование объекта не выполнялось или не было успешно завершено. Системное значение QALWOBJRST допускает восстановление объекта. У выполнявшего операцию пользователя не было специальных прав доступа *ALLOBJ, и уровень защиты системы был не ниже 40. Все права доступа к объекту были аннулированы.</p> <p>С Объект был успешно преобразован. Преобразованная копия была восстановлена в системе.</p> <p>Д Преобразование объекта не выполнялось или не было успешно завершено. Системное значение QALWOBJRST допускает восстановление объекта. У пользователя были специальные права доступа *ALLOBJ. Все права доступа к объекту были сохранены.</p> <p>Е Ошибка при установке системы.</p> <p>F Объект не восстановлен, т.е. формат подписи отличается от формата i5/OS.</p> <p>G При проверке системы обнаружен системный объект без подписи или объект в режиме наследования.</p> <p>Н При проверке системы обнаружен пользовательский объект без подписи.</p> <p>I При проверке системы обнаружено несоответствие объекта и подписи.</p> <p>J При проверке системы не обнаружен сертификат IBM.</p> <p>К При проверке системы обнаружена подпись в недопустимом формате.</p> <p>М Программа выхода внесла изменения в просматриваемый объект</p> <p>X Программа выхода пометила объект как не прошедший просмотр</p>

Таблица 161. Записи журнала AF (ошибка прав доступа) (продолжение). Файл описания полей QASYAFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
186	254	640	Имя задания	Char(10)	Имя задания.
196	264	650	Имя польз.	Char(10)	Имя пользователя задания.
206	274	660	Номер задания	Zoned(6,0)	Номер задания.
212	280	666	Имя программы	Char(10)	Имя программы.
222	290	676	Библиотека программы	Char(10)	Имя библиотеки, в которой расположена программа.
232	300	686	Польз. профайл ²	Char(10)	Имя пользователя, у которого нет необходимых прав доступа.
242	310	696	Имя рабочей станции	Char(10)	Имя рабочей станции или ее типа.
252	320	706	Номер инструкции программы	Zoned(7,0)	Номер инструкции в программе.
259	327	713	Имя поля	Char(10)	Имя поля.
269	337	723	Код нарушения операции	Char(3)	<p>Тип обнаруженного нарушения операции; задается только в том случае, если тип нарушения (J5, смещение 610) равен X.</p> <p>AAC Нет прав доступа для выполнения команды расширенного анализа SST.</p> <p>HCA Пользовательский профайл сервисных средств, у которого нет прав на выполнение операции по настройке аппаратного обеспечения (QYHCHCOP).</p> <p>LIC Значение LIC указывает на то, что исправление Лицензионного внутреннего кода не было применено из-за ошибки в подписи.</p> <p>SFA Нет прав доступа для активации атрибута среды, позволяющего обращаться к системным файлам.</p> <p>CMD Была сделана попытка запустить команду, заблокированную системным администратором.</p>
272	340	726	Польз. Office	Char(10)	Имя пользователя Office.
282	350	736	Имя DLO	Char(12)	Имя объекта библиотеки документов.
294	362	748	(Зарезерв.)	Char(8)	
302	370	756	Путь к папке ^{15, 16}	Char(63)	Полное имя папки.
365	433	819	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
375			(Зарезерв.)	Char(20)	
	443	829	(Зарезерв.)	Char(18)	
	461	847	Длина имени объекта ³	Binary(4)	Длина имени объекта.

Таблица 161. Записи журнала AF (ошибка прав доступа) (продолжение). Файл описания полей QASYAFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
395	463	849	CCSID имени объекта ³	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
399	467	853	ИД страны или региона для имени объекта ³	Char(2)	ИД страны или региона, связанный с именем объекта.
401	469	855	ИД языка для имени объекта ³	Char(3)	ИД языка, связанный с именем объекта.
404	472	858	(Зарезерв.)	Char(3)	
407	475	861	ИД родительского файла ^{3,4}	Char(16)	ИД файла, связанный с родительским каталогом.
423	491	877	ИД файла объекта ^{3,4}	Char(16)	ИД файла объекта.
439	507	893	Имя объекта ^{3,6}	Char(512)	Имя объекта.
	1019	1405	ИД файла объекта ³	Char(16)	ИД файла объекта.
	1035	1421	Имя ASP ¹⁰	Char(10)	Имя ASP.
	1045	1431	Номер ASP ¹⁰	Char(5)	Номер ASP.
	1050	1436	CCSID пути ³	Binary(5)	Идентификатор набора символов, связанный с путем.
I	1054	1440	ИД страны или региона для полного пути ³	Char(2)	ИД страны или региона, связанный с именем пути.
I	1056	1442	ИД языка для полного пути ³	Char(3)	ИД языка, связанный с именем пути.
I	1059	1445	Длина пути ³	Binary(4)	Длина имени пути.
	1061	1447	Индикатор пути ³	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	1062	1448	Отн. ИД каталога ^{3,8}	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ⁸
I	1078	1464	Путь ^{3,9}	Char(5002)	Путь к объекту.
		6466	Имя ASP библиотеки программ	Char(10)	Имя ASP библиотеки программ
		6476	Номер ASP библиотеки программ	Char(5)	Номер ASP библиотеки программ

Таблица 161. Записи журнала AF (ошибка прав доступа) (продолжение). Файл описания полей QASYAFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1					Если задан тип нарушения G, то имя объекта содержит имя библиотеки *SRVPGM, в которой расположена программа выхода, обнаружившая ошибку. Дополнительная информация о типах нарушений приведена в "Записи журнала контроля за действиями" на стр. 285.
2					<p>Данное поле содержит имя пользователя, послужившего причиной создания записи. Библиотека QSYS может быть задана в качестве пользователя в следующих полях:</p> <ul style="list-style-type: none"> • смещение 41 и 118 в записях *TYPE2 • смещение 55 и 132 в записях *TYPE4 • смещение 65 и 187 в записях *TYPE5
3					Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.
4					Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.
5					Если тип нарушения равен T, то в качестве имени объекта будет указан порт TCP/IP, для работы с которым у пользователя нет прав доступа. Значение будет выровнено по левому краю и дополнено справа пробелами. Поля библиотеки и типа объекта будут пустыми.
6					Если тип нарушения равен O, то в поле имени объекта интегрированной файловой системы будет указано имя объекта оптической памяти. Поля ИД страны или региона, ИД языка, ИД родительского каталога и ИД файла объекта будут пустыми.
7					Создаваемый объект класса Java не обязательно расширяет свой базовый класс, так как базовый класс содержит системные атрибуты Java.
8					Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.
9					Это поле переменной длины. Длина пути указывается в первых двух байтах.
10					Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.
11					Если тип нарушения равен X, а значение кода нарушения операции - LIC, значит, из-за ошибки в подписи не было применено исправление Лицензионного внутреннего кода. Данное поле содержит номер исправления Лицензионного внутреннего кода, которое не удалось применить.
12					Если задан тип нарушения K, то в качестве имени объекта указано имя команды или программы, обнаружившей ошибку. Если у команды несколько имен, то имя команды, указанное в контрольной записи, может отличаться от того, что было использовано при запуске команды, однако оно будет эквивалентно ему. Специальное значение *INSTR означает, что ошибку обнаружила машинная инструкция.
13					Если задан тип нарушения K, то в качестве имени библиотеки указано либо имя библиотеки программы, обнаружившей ошибку, либо значение *N в качестве библиотеки команды, обнаружившей ошибку.
14					Если задан тип нарушения K, то в качестве типа объекта указан объектный тип команды или программы, обнаружившей ошибку.
15					Если задан тип нарушения K, то в качестве пути к папке может быть указано полное имя API или точки выхода, обнаруживших ошибку.
16					Если тип нарушения равен X, а значение кода нарушения операции - AAC, то путь к папке будет содержать 30-символьную команду расширенного анализа.
17					Если типа объекта - это *LIC, а библиотека объектов - *N, то именем объекта будет Лицензионный внутренний код Ru.

Записи журнала AP (Принятые права доступа)

В этой таблице представлен формат записей журнала AP (Принятые права доступа)

Таблица 162. Записи журнала AP (Принятые права доступа). Файл описания полей QASYAPJE/J4/J5

Смещ.			Поле	Отформатировать	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	S Запуск E Завершение A Принятые права доступа, которые применялись при активации программы
157	225	611	Имя объекта	Char(10)	Имя программы, служебной программы или пакета SQL
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Польз. профайл владельца	Char(10)	Имя пользовательского профайла, права доступа которого принимаются.
195	263	649	ИД файла объекта	Char(16)	ИД файла объекта.
	279	665	Имя ASP ¹	Char(10)	Имя ASP.
	289	675	Номер ASP ¹	Char(5)	Номер ASP.
¹ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.					

Записи журнала AU (изменение атрибутов)

В этой таблице представлен формат записей журнала AU (изменение атрибутов).

Таблица 163. Записи журнала AU (изменение атрибутов). Файл описания полей QASYAUJ5

Смещ.		Поле	Отформатировать	Описание
J5				
610		Тип записи	Char(1)	Тип записи. E Атрибуты конфигурации EIM
611		Действие	Char(3)	Действие CHG Изменение атрибутов
614		ФИО	Char(100)	Имя атрибута

Таблица 163. Записи журнала AU (изменение атрибутов) (продолжение). Файл описания полей QASYAUJ5

Смещ.		Поле	Отформатировать	Описание
J5				
714		Длина нового значения	Binary(4)	Длина нового значения
716		CCSID нового значения	Binary(5)	CCSID нового значения
720		ИД страны или региона для нового значения	Char(2)	ИД страны или региона для нового значения
722		ИД языка для нового значения	Char(3)	ИД языка для нового значения
725		Новое значение	Char(2002) ¹	Новое значение
2727		Длина прежнего значения	Binary(4)	Длина прежнего значения
2729		CCSID прежнего значения	Binary(5)	CCSID прежнего значения
2733		ИД страны или региона для прежнего значения	Char(2)	ИД страны или региона для прежнего значения
2735		ИД языка для прежнего значения	Char(3)	ИД языка для прежнего значения
2738		Старое значение	Char(2002) ¹	Прежнее значение
1 Это поле переменной длины. Длина поля указывается в первых двух байтах.				

Записи журнала SA (изменение прав доступа)

В этой таблице представлен формат записей журнала SA (изменение прав доступа)

Таблица 164. Записи журнала SA (изменение прав доступа). Файл описания полей QASYCAJE/J4/J5

Смещ.			Поле	Отформатировать	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение прав доступа
157	225	611	Имя объекта	Char(10)	Имя объекта.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.

Таблица 164. Записи журнала SA (изменение прав доступа) (продолжение). Файл описания полей QASYCAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
185	253	639	Имя польз.	Char(10)	Имя пользовательского профайла, права доступа которого предоставляются или аннулируются.
195	263	649	Список прав доступа	Char(10)	Имя списка прав доступа.
					Предоставляемые или аннулируемые права доступа:
205	273	659	Существование объекта	Char(1)	Д *OBJEXIST
206	274	660	Управление объектом	Char(1)	Д *OBJMGT
207	275	661	Операционные права доступа к объекту	Char(1)	Д *OBJOPR
208	276	662	Управление списком прав доступа	Char(1)	Д *AUTLMGT
209	277	663	Список прав доступа	Char(1)	Д Общие права доступа *AUTL
210	278	664	Права на чтение	Char(1)	Д *READ
211	279	665	Права на добавление	Char(1)	Д *ADD
212	280	666	Права на обновление	Char(1)	Д *UPD
213	281	667	Права на удаление	Char(1)	Д *DLT
214	282	668	Исключающие права доступа	Char(1)	Д *EXCLUDE
215	283	669	Права на выполнение	Char(1)	Д *EXECUTE
216	284	670	Права на изменение атрибутов объекта	Char(1)	Д *OBJALTER
217	285	671	Права на обращение к объекту	Char(1)	Д *OBJREF
218	286	672	(Зарезерв.)	Char(4)	
222	290	676	Тип команды	Char(3)	Тип указанной команды. GRT Предоставление прав RPL Предоставление прав с заменой существующих RVK Аннулирование прав USR Операция GRTUSRAUT
225	293	679	Имя поля	Char(10)	Имя поля.

Таблица 164. Записи журнала СА (изменение прав доступа) (продолжение). Файл описания полей QASYCAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
235	303		(Зарезерв.)	Char(10)	
		689	Атрибут объекта	Char(10)	Атрибут объекта.
245	313	699	Польз. Office	Char(10)	Имя пользователя Office.
255	323	709	Имя DLO	Char(12)	Имя объекта библиотеки документов.
267	335	721	(Зарезерв.)	Char(8)	
275	343	729	Полное имя папки	Char(63)	Полное имя папки.
338	406	792	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
348	416	802	Состояние пользователя	Char(1)	Д Состояние пользователя изменено
349	417	803	Код доступа	Char(1)	А Код доступа добавлен Ч Код доступа удален
350	418	804	Код доступа	Char(4)	Код доступа.
354			(Зарезерв.)	Char(20)	
	422	808	(Зарезерв.)	Char(18)	
	440	826	Длина имени объекта ¹	Binary(4)	Длина имени объекта.
374	442	828	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
378	446	832	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
380	448	834	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
383	451	837	(Зарезерв.)	Char(3)	
386	454	840	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
402	470	856	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
418	486	872	Имя объекта ¹	Char(512)	Имя объекта.
	998	1384	ИД файла объекта	Char(16)	ИД файла объекта.
	1014	1400	Имя ASP ⁵	Char(10)	Имя ASP.
	1024	1410	Номер ASP ⁵	Char(5)	Номер ASP.
	1029	1415	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	1033	1419	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.

Таблица 164. Записи журнала SA (изменение прав доступа) (продолжение). Файл описания полей QASYCAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1035	1421	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	1038	1424	Длина пути	Binary(4)	Длина имени пути.
	1040	1426	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	1041	1427	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1057	1443	Путь ⁴	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁵ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала CD (командная строка)

В этой таблице представлен формат записей журнала CD (командная строка).

Таблица 165. Записи журнала CD (командная строка). Файл описания полей QASYCDJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.

Таблица 165. Записи журнала CD (командная строка) (продолжение). Файл описания полей QASYCDJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Тип записи	Char(1)	Тип записи. C Выполнение команды L Оператор OCL O Команда управления в операторе P Процедура S/36 S Запуск команды после подстановки команды U Оператор управления утилитой
157	225	611	Имя объекта	Char(10)	Имя объекта.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Запуск из программы на CL	Char(1)	Д Да Нет Нет
186	254	640	Строка команды	Char(6000)	Запущенная команда, включая все ее параметры.
		6640	Имя ASP библиотеки команды	Char(10)	Имя ASP библиотеки команды
		6650	Номер ASP библиотеки команды	Char(5)	Номер ASP библиотеки команды

Записи журнала CO (создание объекта)

В этой таблице представлен формат записей журнала CO (создание объекта)

Таблица 166. Записи журнала CO (создание объекта). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. Нет Создание нового объекта Ч Замена существующего объекта
157	225	611	Имя объекта	Char(10)	Имя объекта.

Таблица 166. Записи журнала СО (создание объекта) (продолжение). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, в которой расположен объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253		(Зарезерв.)	Char(20)	
		639	Атрибут объекта	Char(10)	Атрибут объекта.
		649	(Зарезерв.)	Char(10)	
205	273	659	Польз. Office	Char(10)	Имя пользователя Office.
215	283	669	Имя DLO	Char(12)	Имя объекта библиотеки документов.
227	295	681	(Зарезерв.)	Char(8)	
235	303	689	Полное имя папки	Char(63)	Полное имя папки.
298	366	752	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
308			(Зарезерв.)	Char(20)	
	376	762	(Зарезерв.)	Char(18)	
	394	780	Длина имени объекта	Binary(4)	Длина имени объекта.
328	396	782	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
332	400	786	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
334	402	788	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
337	405	791	(Зарезерв.)	Char(3)	
340	408	794	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
356	424	810	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
372	440	826	Имя объекта ¹	Char(512)	Имя объекта.
	952	1338	ИД файла объекта	Char(16)	ИД файла объекта.
	968	1354	Имя ASP ⁵	Char(10)	Имя ASP.
	978	1364	Номер ASP ⁵	Char(5)	Номер ASP.
	983	1369	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	987	1373	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	989	1375	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.

Таблица 166. Записи журнала CO (создание объекта) (продолжение). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	992	1378	Длина пути	Binary(4)	Длина имени пути.
	994	1380	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	995	1381	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1011	1397	Путь ⁴	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁵ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала CP (изменение пользовательского профайла)

В этой таблице представлен формат записей журнала CP (изменение пользовательского профайла).

Таблица 167. Записи журнала CP (изменение пользовательского профайла). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение пользовательского профайла
157	225	611	Имя пользовательского профайла	Char(10)	Имя измененного пользовательского профайла.

Таблица 167. Записи журнала CP (изменение пользовательского профиля) (продолжение). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	256	639	Команда	Char(3)	Тип указанной команды. CRT CRTUSRPRF CHG CHGUSRPRF RST RSTUSRPRF DST Сброс пароля QSECOFR с помощью DST RPA API QSYRESPA
188	256	642	Изменен пароль	Char(1)	Д Пароль изменен
189	257	643	Пароль *NONE	Char(1)	Д Пароль равен *NONE.
190	258	644	Истек срок действия пароля	Char(1)	Д Срок действия пароля истек Нет Срок действия пароля не истек
191	259	645	Специальные права доступа ко всем объектам	Char(1)	Д *ALLOBJ, специальные права доступа
192	260	646	Специальные права на управление заданиями	Char(1)	Д Специальные права доступа *JOBCTL
193	261	647	Специальные права на сохранение системы	Char(1)	Д Специальные права доступа *SAVSYS
194	262	648	Специальные права доступа администратора защиты	Char(1)	Д Специальные права доступа *SECADM
195	263	649	Специальные права на управление буфером	Char(1)	Д Специальные права доступа *SPLCTL
196	264	650	Специальные служебные права доступа	Char(1)	Д Специальные права доступа *SERVICE
197	265	651	Специальные права на контроль	Char(1)	Д Специальные права доступа *AUDIT
198	266	652	Специальные права доступа к конфигурации системы	Char(1)	Д Специальные права доступа *IOSYSCFG
199	267	653	(Зарезерв.)	Char(13)	

Таблица 167. Записи журнала CP (изменение пользовательского профайла) (продолжение). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
212	280	666	Профайл группы	Char(10)	Имя профайла группы.
222	290	676	Владелец	Char(10)	Владелец объектов, входящий в состав профайла группы.
232	300	686	Права доступа группы	Char(10)	Права доступа группы.
242	310	696	Начальная программа	Char(10)	Имя начальной программы пользователя.
252	320	706	Библиотека начальной программы	Char(10)	Имя библиотеки, в которой расположена начальная программа.
262	330	716	Начальное меню	Char(10)	Имя начального меню пользователя.
272	340	726	Библиотека начального меню	Char(10)	Имя библиотеки, в которой расположено начальное меню.
282	350	736	Текущая библиотека	Char(10)	Имя текущей библиотеки пользователя.
292	360	746	Ограничить возможности	Char(10)	Значение параметра ограничения возможностей.
302	370	756	Класс пользователя	Char(10)	Класс, к которому относится данный пользователь.
312	380	766	Ограничение приоритета	Char(1)	Значение параметра ограничения приоритета.
313	381	767	Состояние профайла	Char(10)	Состояние пользовательского профайла.
323	391	777	Тип прав доступа группы	Char(10)	Значение параметра GRPAUTTYT.
333	401	787	Доп. профайлы групп	Char(150)	До 15 имен дополнительных профайлов групп данного пользователя.
483	551	937	ИД пользователя	Char(10)	Идентификатор пользователя.
493	561	947	ИД группы	Char(10)	Идентификатор группы.
503	571	957	Локальное управление паролем	Char(10)	Значение параметра LCLPDMGT.

Таблица 167. Записи журнала CP (изменение пользовательского профиля) (продолжение). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		967	Соответствие правилам составления паролей	Char(10)	<p>Указывает, соответствует ли новый пароль правилам составления паролей.</p> <p>*PASSED Проверен и соответствует.</p> <p>*SYSVAL Проверен, но не соответствует из-за правила, основанного на системном значении.</p> <p>*EXITPGM Проверен, но не соответствует из-за ответа программы выхода.</p> <p>*NONE Не проверен; в качестве нового пароля указано значение *NONE.</p> <p>*NOCHECK Не проверен; пароль был изменен.</p> <p>Это поле имеет смысл только в том случае, когда в поле Изменен пароль указано Y.</p>
		977	Срок действия пароля	Char(7)	<p>Указывает новый срок действия пароля.</p> <p>*NOMAX Срок действия не ограничен.</p> <p>*SYSVAL Применяется системное значение QPWDEXPTV.</p> <p>number Срок действия в днях.</p>
		984	Блокировка изменения пароля	Char(10)	<p>Указывает новое значение блокировки изменения пароля.</p> <p>*SYSVAL Применяется системное значение QPWDCHGBLK.</p> <p>*NONE Блокировка выключена.</p> <p>1-99 Часы блокировки.</p>

Записи журнала CQ (изменение *CRQD)

В этой таблице представлен формат записей журнала CQ (изменение *CRQD).

Таблица 168. Записи журнала CQ (изменение *CRQD). Файл описания полей QASYCOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение объекта *CRQD
157	225	611	Имя объекта	Char(10)	Имя измененного объекта.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки объекта.
177	245	631	Тип объекта	Char(8)	Тип объекта.
		639	Имя ASP	Char(10)	Имя ASP библиотеки CRQD
		649	Номер ASP	Char(5)	Номер ASP библиотеки CRQD

Записи журнала CU (операции с кластерами)

В этой таблице представлен формат записей журнала CU (операции с кластерами).

Таблица 169. Записи журнала CU (операции с кластерами). Файл описания полей QASYCOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.
	224	610	Тип записи	Char(1)	Тип записи. M Операция управления кластером Ч Операция управления группой ресурсов кластера (*GRP)

Таблица 169. Записи журнала CU (операции с кластерами) (продолжение). Файл описания полей QASYCOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	225	611	Действие записи	Char(3)	Тип действия. ADD Добавление CRT Создание DLT Удаление DST Рассылка END Завершение FLO Восстановление после сбоя LST Просмотр сведений RMV Удаление STR Запуск SWT Коммутатор UPC Обновление атрибутов
	228	614	Состояние	Char(3)	Состояние запроса. ABN Обработка запроса завершена аварийно AUT Нет необходимых прав доступа; требуются специальные права *IOSYSCFG END Запрос успешно обработан STR Запущена обработка запроса
	231	617	Имя объекта CRG	Char(10)	Имя объекта группы ресурсов кластера. Прим.: Значение в этом поле задается только для записей типа R.
	241	627	Имя библиотеки CRG	Char(10)	Библиотека объекта группы ресурсов кластера. Прим.: Значение в этом поле задается только для записей типа R.
	251	637	Имя кластера	Char(10)	Имя кластера.
	261	647	ИД узла	Char(8)	ИД узла.
	269	655	ИД исходного узла	Char(8)	ИД исходного узла.
	277	663	Имя исходного пользователя	Char(10)	Имя пользователя исходной системы, запустившего запрос.
	287	673	Имя польз. очереди	Char(10)	Имя пользовательской очереди, в которую отправляются ответы.
	297	683	Библиотека польз. очереди	Char(10)	Библиотека пользовательской очереди.
		693	Имя ASP	Char(10)	Имя ASP библиотеки пользовательской очереди
		703	Номер ASP	Char(5)	Номер ASP библиотеки пользовательской очереди

Записи журнала CV (проверка соединения)

В этой таблице представлен формат записей журнала CV (проверка соединения).

Таблица 170. Записи журнала CV (проверка соединения). Файл описания полей QASYCOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.
	224	610	Тип записи	Char(1)	<p>Тип записи.</p> <p>С Соединение установлено</p> <p>Е Соединение завершено</p> <p>Ч Соединение отклонено</p>
	225	611	Действие	Char(1)	<p>Действие для соединений данного типа.</p> <p>" " Соединение успешно установлено или завершено. Применяется для записей типов С и Е.</p> <p>А Узел не был идентифицирован. Применяется для записей типов R и Е.</p> <p>С Сервер идентификации не отвечает. Применяется для записей типа R.</p> <p>L Ошибка в конфигурации LCP. Применяется для записей типа R.</p> <p>Нет Ошибка в конфигурации NCP. Применяется для записей типа R.</p> <p>P Неверный пароль. Применяется для записей типов R и Е.</p> <p>Ч Узел отклонил запрос на идентификацию. Применяется для записей типа R.</p> <p>T Ошибка в конфигурации L2TP. Применяется для записей типов R и Е.</p> <p>U Недопустимое имя пользователя. Применяется для записей типов R и Е.</p>
	226	612	Имя профайла двухточечного соединения	Char(10)	Имя профайла двухточечного соединения
	236	622	Протокол	Char(10)	<p>Тип записи.</p> <p>L2TP Протокол L2TP</p> <p>PPP Двухточечный протокол.</p> <p>SLIP Протокол подключения к Internet по последовательной линии.</p>

Таблица 170. Записи журнала CV (проверка соединения) (продолжение). Файл описания полей QASYCOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	246	632	Способ идентификации в локальной системе.	Char(10)	Тип записи. CHAP Протокол идентификации с квитированием связи по вызову. PAP Протокол идентификации по паролю. SCRIPT Идентификация по сценарию.
	256	642	Способ идентификации в удаленной системе	Char(10)	Тип записи. CHAP Протокол идентификации с квитированием связи по вызову. PAP Протокол идентификации по паролю. RADIUS Идентификация Radius. SCRIPT Идентификация по сценарию.
	266	652	Имя объекта	Char(10)	Имя объекта *VLDL.
	276	662	Имя библиотеки	Char(10)	Имя библиотеки объекта *VLDL.
	286	672	Имя пользователя *VLDL	Char(100)	Имя пользователя *VLDL.
	386	772	Локальный IP-адрес	Char(40)	IP-адрес локальной системы.
	426	812	Удаленный IP-адрес	Char(40)	IP-адрес удаленной системы.
	466	852	Пересылка пакетов IP	Char(1)	Тип записи. Д Пересылка пакетов IP включена. Нет Пересылка пакетов IP выключена.

Таблица 170. Записи журнала CV (проверка соединения) (продолжение). Файл описания полей QASYCOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	467	853	Прогу ARP	Char(1)	Тип записи. Д Функция Proxu ARP включена. Нет Функция Proxu ARP выключена.
	468	854	Имя Radius	Char(10)	Имя профайла AAA.
	478	864	IP-адрес системы, выполняющей идентификацию	Char(40)	IP-адрес системы, выполняющей идентификацию.
	518	904	ИД сеанса учетной записи	Char(14)	ИД сеанса учетной записи.
	532	918	ИД сеансов учетной записи	Char(14)	ИД сеансов учетной записи.
	546	932	Счетчик ссылок учетной записи	Binary(4)	Счетчик ссылок учетной записи.
	548	934	Тип туннеля	Char(1)	Тип туннеля: 0 Туннель не применяется 3 L2TP 6 АН 9 ESP
	549	935	Клиент туннеля	Char(40)	Клиент туннеля.
	589	975	Сервер туннеля	Char(40)	Сервер туннеля.
	629	1015	Время сеанса учетной записи	Char(8)	Время сеанса учетной записи. Применяется для записей типов R и E.
	637	1023	Зарезерв.	Binary(4)	Всегда нуль
		1025	Имя ASP	Char(10)	Имя ASP библиотеки контрольного списка
		1035	Номер ASP	Char(5)	Номер ASP библиотеки контрольного списка

Записи журнала СУ (настройка шифрования)

В этой таблице представлен формат записей журнала СУ (настройка шифрования).

Таблица 171. Записи журнала СУ (настройка шифрования). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 171. Записи журнала СУ (настройка шифрования) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	224	610	Тип записи	Char(1)	<p>Тип записи.</p> <p>A Функция управления доступом к шифровальному сопроцессору</p> <p>F Функция управления шифровальным сопроцессором</p> <p>K Функция главного ключа шифровальных служб</p> <p>M Функция главного ключа шифровального сопроцессора</p>
	225	611	Действие	Char(3)	<p>Выполнена следующая функция настройки шифрования:</p> <p>CCP Определен профайл карты.</p> <p>CCR Определена роль карты.</p> <p>CLK Установлено время на часах.</p> <p>CLR Удалены главные ключи.</p> <p>CRT Созданы главные ключи.</p> <p>DCP Удален профайл карты.</p> <p>DCR Удалена роль карты.</p> <p>DST Разосланы главные ключи.</p> <p>EID Задан ИД среды.</p> <p>FCV Загружен или очищен FCV.</p> <p>INI Повторно инициализирована карта.</p> <p>LOD Загружен главный ключ.</p> <p>QRY Запрошена информация о роли или профайле.</p> <p>RCP Заменен профайл карты.</p> <p>RCR Заменена роль карты.</p> <p>RCV Получены главные ключи.</p> <p>SET Заданы главные ключи.</p> <p>SHR Продублированы общие ресурсы.</p> <p>TST Проверен главный ключ.</p>
	228	614	Профайл карты	Char(8)	Имя профайла карты. ²
	236	622	Роль карты	Char(8)	Роль профайла карты. ²
	244	630	Имя устройства	Char(10)	Имя шифровального устройства. ²

Таблица 171. Записи журнала СУ (настройка шифрования) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		640	ИД главного ключа ¹	Binary(4)	ИД главного ключа шифровальных служб ³ . Возможны следующие значения: -2 Главный ключ сохранения/ восстановления -1 Главный ключ ASP 1 Главный ключ 1 2 Главный ключ 2 3 Главный ключ 3 4 Главный ключ 4 5 Главный ключ 5 6 Главный ключ 6 7 Главный ключ 7 8 Главный ключ 8
		644	Шифрование главного ключа	Char(1)	Главный ключ, зашифрованный главным ключом C/B. Д Главный ключ задан и зашифрован главным ключом сохранения/ восстановления по умолчанию. Нет Главный ключ задан и зашифрован главным ключом сохранения/ восстановления, указанным пользователем.
		645	Версия главного ключа	Char(8)	Версия главного ключа, которая была очищена. NEW Очищена новая версия. CURRENT Очищена текущая версия. OLD Очищена прежняя версия. PENDING Очищена ожидающая версия.
¹ Если тип записи равен "К", то в качестве профайла карты (J5, смещение 614), роли карты (J5, смещение 622) и имени устройства (J5, смещение 630) указаны пробелы. ² Если тип записи равен К, то это поле пустое. ³ Если тип записи не равен К, то это поле пустое.					

Записи журнала DI (сервер каталогов)

В этой таблице представлен формат записей журнала DI (сервер каталогов).

Таблица 172. Записи журнала DI (сервер каталогов). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
	224	610	Тип записи	Char(1)	Тип записи. L Операция LDAP
	225	611	Тип операции	Char(2)	Тип операции LDAP: AD Изменение атрибута контроля. AF Недостаточные права доступа. BN Успешная операция связывания. CA Изменение прав доступа ко объекту. CF Изменение конфигурации. CI Создание экземпляра CO Создание объекта. CP Изменение пароля. DI Удаление экземпляра DO Удаление объекта. EX Экспорт каталога LDAP. IM Импорт каталога LDAP. OM Управление объектом (переименование). OW Изменение принадлежности. PO Изменение стратегии. PW Неверный пароль. RM Управление копированием. UB Успешное аннулирование связывания. ZC Изменение объекта. ZR Чтение объекта.

Таблица 172. Записи журнала DI (сервер каталогов) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатированно	Описание
JE	J4	J5			
	227	613	Код ошибки прав доступа	Char(1)	<p>Код ошибки прав доступа. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен AF.</p> <p>A Попытка несанкционированного изменения значения контроля.</p> <p>B Попытка несанкционированного связывания.</p> <p>C Попытка несанкционированного создания объекта.</p> <p>D Попытка несанкционированного удаления объекта.</p> <p>E Попытка несанкционированного экспорта.</p> <p>F Попытка несанкционированного изменения конфигурации (администратора, протокола изменений, библиотеки базы данных, копий, параметров публикации).</p> <p>G Попытка несанкционированного управления копированием.</p> <p>I Попытка несанкционированного импорта.</p> <p>M Попытка несанкционированного изменения.</p> <p>P Попытка несанкционированного изменения стратегии.</p> <p>Ч Попытка несанкционированного чтения (поиска).</p> <p>U Попытка несанкционированного чтения конфигурации контроля.</p> <p>X Попытка несанкционированного управления доступом к ргоху.</p>

Таблица 172. Записи журнала DI (сервер каталогов) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатированное	Описание
JE	J4	J5			
	228	614	Изменение конфигурации	Char(1)	<p>Тип изменения конфигурации. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен CF.</p> <p>A Изменение ND администратора.</p> <p>C Изменение параметров входа в систему или выхода из нее.</p> <p>L Изменение имени библиотеки базы данных.</p> <p>P Изменение агента публикации.</p> <p>Ч Изменение сервера-копии.</p> <p>Если тип операции (J5, смещение 611) равен RM, то могут быть указаны следующие значения:</p> <p>U Приостановить копирование.</p> <p>V Возобновить копирование.</p> <p>W Скопировать ожидающие изменения сейчас.</p> <p>X Пропустить одно или несколько ожидающих изменений.</p> <p>Д Стабилизировать контекст копирования.</p> <p>Z Дестабилизировать контекст копирования.</p>
	229	615	Код изменения конфигурации	Char(1)	<p>Код изменения конфигурации. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен CF.</p> <p>A Добавление элемента конфигурации</p> <p>D Удаление элемента конфигурации</p> <p>M Изменение элемента</p>
	230	616	Флаг наследования	Char(1)	<p>Задаёт новое значение параметра наследования владельца или ACL. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен CA или OW.</p> <p>T Истина</p> <p>F Ложь</p>
	231	617	Способ идентификации при связывании	Char(20)	<p>Способ идентификации при связывании. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен BN.</p>
	251	637	Версия LDAP	Char(4)	<p>Версия клиента, отправившего запрос. Это поле задается только в том случае, если операция выполняется с помощью сервера LDAP.</p> <p>2 LDAP версии 2</p> <p>3 LDAP версии 3</p>

Таблица 172. Записи журнала DI (сервер каталогов) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	255	641	Индикатор SSL	Char(1)	Указывает, применялся ли SSL при обработке запроса. Это поле задается только в том случае, если операция выполняется с помощью сервера LDAP. 0 Нет 1 Да
	256	642	Тип запроса	Char(1)	Тип запроса. Это поле задается только в том случае, если операция выполняется с помощью сервера LDAP. A Идентифицированный Нет Анонимный U Неидентифицированный
	257	643	ИД соединения	Char(20)	ИД соединения запроса. Это поле задается только в том случае, если операция выполняется с помощью сервера LDAP.
	277	663	IP-адрес клиента	Char(50)	IP-адрес и номер порта запроса клиента. Это поле задается только в том случае, если операция выполняется с помощью сервера LDAP.
	327	713	CCSID имени пользователя	Bin(5)	Идентификатор набора символов, связанный с именем пользователя.
	331	717	Длина имени пользователя	Bin(4)	Длина имени пользователя.
	333	719	Имя пользователя ¹	Char(2002)	Имя пользователя LDAP.
	2335	2721	CCSID имени объекта	Bin(5)	Идентификатор набора символов, связанный с именем объекта.
	2339	2725	Длина имени объекта	Bin(4)	Длина имени объекта.
	2341	2727	Имя объекта ¹	Char(2002)	Имя объекта LDAP.
	4343	4729	CCSID имени владельца	Bin(5)	Идентификатор набора символов, связанный с именем владельца. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен OW.
	4347	4733	Длина имени владельца	Bin(4)	Длина имени владельца. Это поле задается только в том случае, если тип операции равен OW.
	4349	4735	Имя владельца ¹	Char(2002)	Имя владельца. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен OW.

Таблица 172. Записи журнала DI (сервер каталогов) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатированное	Описание
JE	J4	J5			
	6351	6737	CCSID нового имени	Bin(5)	Идентификатор набора символов, связанный с новым именем. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен OM, OW, PO, ZC, AF+M или AF+P. <ul style="list-style-type: none"> Для операций типа OM это поле содержит CCSID нового имени объекта. Для операций типа OW данное поле содержит CCSID нового имени владельца. Для операций типов PO, ZC, AF+M и AF+P это поле содержит CCSID списка типов измененных атрибутов из поля Новое имя.
	6355	6741	Длина нового имени	Bin(4)	Длина нового имени. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен OM, OW, PO, ZC, AF+M или AF+P. <ul style="list-style-type: none"> Для операций типа OM это поле содержит длину нового имени объекта. Для операций типа OW данное поле содержит длину нового имени владельца. Для операций типов PO, ZC, AF+M и AF+P это поле содержит длину списка типов измененных атрибутов из поля Новое имя.
	6357	6743	Новое имя ¹	Char(2002)	Новое имя. Это поле задается только в том случае, если тип операции (J5, смещение 611) равен OM, OW, PO, ZC, AF+M или AF+P. <ul style="list-style-type: none"> Для операций типа OM это поле содержит новое имя объекта. Для операций типа OW данное поле содержит новое имя владельца. Для операций типов PO, ZC, AF+M и AF+P это поле содержит список типов измененных атрибутов.
	8359	8745	ИД файла объекта ²	Char(16)	ИД файла экспортируемого объекта.
	8375	8761	Имя ASP ²	Char(10)	Имя ASP.
	8385	8771	Номер ASP ²	Char(5)	Номер ASP.
	8390	8776	CCSID пути ²	Bin(5)	Идентификатор набора символов, связанный с путем.
	8394	8780	ИД страны или региона для полного пути ²	Char(2)	ИД страны или региона, связанный с именем пути.
	8396	8782	ИД языка для полного пути ²	Char(3)	ИД языка, связанный с именем.
	8399	8785	Длина пути ²	Bin(4)	Длина имени пути.

Таблица 172. Записи журнала DI (сервер каталогов) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
	8401	8787	Индикатор пути ²	Char(1)	Индикатор пути. Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	8402	8788	Отн. ИД каталога ^{2,3}	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	8418	8804	Путь ^{1,2}	Char(5002)	Путь к объекту.
		13806	Локальный польз. профайл	Char(10)	Имя локального пользовательского профайла, который связан с именем пользователя LDAP (J5, смещение 719). Пустое поле означает, что нет связанного пользовательского профайла.
		13816	Индикатор администратора	Char(1)	Индикатор администратора для имени пользователя LDAP (J5, смещение 719). Д Пользователь LDAP является администратором. Нет Пользователь LDAP не является администратором. U В данный момент неизвестно, является ли пользователь LDAP администратором.
		13817	CCSID ИД проху	Bin(5)	Идентификатор набора символов (CCSID) ИД проху.
I		13821	Длина ИД проху	Bin(4)	Длина ИД проху.
I		13823	ИД проху ¹	Char(2002)	ИД проху. Это поле используется, когда для того, чтобы запросить выполнение операции с правами доступа ИД проху или выполнить связывание SASL, в котором клиент указал ИД авторизации, отличный от ИД связывания, применяется управление доступом к проху.
I		15825	Подтверждение группы	Char(1)	Подтверждение членства в группе 0 Группы не были указаны клиентом. 1 Группы были указаны клиентом.
I		15826	Перекрестная ссылка	Char(36)	Строка перекрестной ссылки, применяемая для связи этой записи с записями XD перечня групп.
I		15862	Имя экземпляра	Char(8)	Имя экземпляра
I		15870	CCSID маршрута	Bin(5)	CCSID маршрута
I		15874	Длина маршрута	Bin(4)	Длина маршрута

Таблица 172. Записи журнала DI (сервер каталогов) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		15876	Маршрут	Char(502)	Запрос маршрута
1	Это поле переменной длины. Первые два байта содержат длину значения поля.				
2	Эти поля задаются только для операций типов (J5, смещение 611) EX и IM.				
3	Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.				

Записи журнала DO (операция удаления)

В этой таблице представлен формат записей журнала DO (операция удаления).

Таблица 173. Записи журнала DO (операция удаления). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Объект был удален не в режиме управления фиксацией C Зафиксированное ожидающее удаление объекта. D Отменено ожидающее создание объекта. I Инициализация пространства переменных среды P Ожидающее удаление объекта (удаление выполнено в режиме управления фиксацией) Ч Отменено ожидающее удаление объекта.
157	225	611	Имя объекта	Char(10)	Имя объекта.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253		(Зарезерв.)	Char(20)	
		639	Атрибут объекта	Char(10)	Атрибут объекта.
		649	(Зарезерв.)	Char(10)	
205	273	659	Польз. Office	Char(10)	Имя пользователя Office.

Таблица 173. Записи журнала DO (операция удаления) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
215	283	669	Имя DLO	Char(12)	Имя объекта библиотеки документов.
227	295	681	(Зарезерв.)	Char(8)	
235	303	689	Полное имя папки	Char(63)	Полное имя папки.
298	366	752	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
308			(Зарезерв.)	Char(20)	
	376	762	(Зарезерв.)	Char(18)	
	394	780	Длина имени объекта ¹	Binary(4)	Длина имени объекта.
328	396	782	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
332	400	786	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
334	402	788	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
337	405	791	(Зарезерв.)	Char(3)	
340	408	794	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
356	424	810	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
372	440	826	Имя объекта ¹	Char(512)	Имя объекта.
	952	1338	ИД файла объекта	Char(16)	ИД файла объекта.
	968	1354	Имя ASP ⁵	Char(10)	Имя ASP.
	978	1364	Номер ASP ⁵	Char(5)	Номер ASP.
	983	1369	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	987	1373	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	989	1375	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	992	1378	Длина пути	Binary(4)	Длина имени пути.
	994	1380	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.

Таблица 173. Записи журнала DO (операция удаления) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	995	1381	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1011	1397	Путь ⁴	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁵ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала DS (сброс поставляемого IBM ИД пользователя сервисных средств)

В этой таблице представлен формат записей журнала DS (сброс поставляемого IBM ИД пользователя сервисных средств).

Таблица 174. Записи журнала DS (сброс поставляемого IBM ИД пользователя сервисных средств). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Сброс пароля ИД пользователя сервисных средств. C Изменение ИД пользователя сервисных средств. P Изменение пароля ИД пользователя сервисных средств.
157	225	611	Сброс поставляемого IBM ИД пользователя сервисных средств	Char(1)	D Запрос на сброс поставляемого IBM ИД пользователя сервисных средств.

Таблица 174. Записи журнала DS (сброс поставляемого IBM ИД пользователя сервисных средств) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
158	226	612	Тип ИД пользователя сервисных средств	Char(10)	Тип ИД пользователя сервисных средств *SECURITY *FULL *BASIC
168	236	622	Новый ИД пользователя сервисных средств	Char(8)	Имя пользователя сервисных средств.
176	244	630	Изменение пароля пользователя сервисных средств	Char(1)	Запрос на изменение пароля пользователя сервисных средств. Д Запрос на изменение пароля пользователя сервисных средств.
	245	631	Новый ИД пользователя сервисных средств	Char(10)	Имя пользователя сервисных средств.
	255	641	Профайл пользователя сервисных средств, отправившего запрос	Char(10)	Имя пользователя сервисных средств, отправившего запрос на изменение.

Записи журнала EV (переменная среды)

В этой таблице представлен формат записей журнала EV (переменная среды).

Таблица 175. Записи журнала EV (переменная среды). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 175. Записи журнала EV (переменная среды) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	224	610	Тип записи	Char(1)	Тип записи. A Добавление C Изменение D Удаление I Инициализация пространства переменных среды
	225	611	Усеченное имя	Char(1)	Указывает, является ли имя переменной среды (смещение 232) усеченным. Д Имя переменной среды усечено. Нет Имя переменной среды не усечено.
	226	612	CCSID	Binary(5)	CCSID имени переменной среды.
	230	616	Длина	Binary(4)	Длина имени переменной среды.
	232	618	Имя переменной среды ²	Char(1002)	Имя переменной среды.
	1234	1620	Новое имя усечено ¹	Char(1)	Указывает, является ли усеченным новое имя переменной среды (смещение 1241). Д Значение переменной среды усечено. Нет Значение переменной среды не усечено.
	1235	1621	CCSID нового имени ¹	Binary(5)	CCSID нового имени переменной среды.
	1239	1625	Длина нового имени ¹	Binary(4)	Длина нового имени переменной среды.
	1241	1627	Новое имя переменной среды ^{1,2}	Char(1002)	Новое имя переменной среды.
¹ Эти поля задаются для записей типа C. ² Это поле переменной длины. Первые два байта содержат длину имени переменной среды.					

Записи журнала GR (шаблон записи)

В этой таблице представлен формат записей журнала GR (шаблон записи)

Таблица 176. Записи журнала GR (шаблон записи). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.

Таблица 176. Записи журнала GR (шаблон записи) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	224	610	Тип записи	Char(1)	Тип записи. A Добавлена программа выхода C Операции управления и отслеживания ресурсов D Удалена программа выхода F Операции регистрации функций Ч Замещена программа выхода
	225	611	Действие	Char(2)	Выполненное действие. ZC Изменение ZR Чтение
	227	613	Имя польз.	Char(10)	Пользовательский профайл Для записей типа F данное поле содержит имя пользователя, для которого была зарегистрирована функция.
	237	623	CCSID поля 1	Binary (5)	Значение CCSID для поля 1.
	241	627	Длина поля 1	Binary (4)	Длина данных в поле 1.

Таблица 176. Записи журнала GR (шаблон записи) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	243	629	Поле 1	Char (102) ¹	<p>Данные поля 1</p> <p>Для записей типа F данное поле содержит описание выполненной операции регистрации функции. Возможные значения:</p> <p>*REGISTER: Функция была зарегистрирована</p> <p>*REREGISTER: Функция была обновлена</p> <p>*DEREGISTER: Аннулирована регистрация функции</p> <p>*CHGUSAGE: Изменена информация о правах доступа к функции</p> <p>*CHKUSAGE: Были проверены права доступа пользователя к функции - проверка прошла успешно</p> <p>*USAGEFAILURE: Были проверены права доступа пользователя к функции - проверка завершилась неудачно</p> <p>Для записей типов A, D и R данное поле содержит сведения о программе выхода для выполненной функции.</p> <p>Для записей типа C это поле содержит имя функции RMC, которую попытался запустить пользователь. Возможны следующие значения:</p> <ul style="list-style-type: none"> • mc_reg_event_select Регистрация события путем выбора атрибутов • mc_reg_event_handle Регистрация события с помощью ссылки на ресурс • mc_reg_class_event Регистрация события для класса ресурсов • mc_unreg_event Отмена регистрации события • mc_define_resource Определение нового ресурса • mc_undefine_resource Удаление определения ресурса • mc_set_select Настройка атрибутов ресурса путем выбора атрибутов • mc_set_handle Настройка атрибутов ресурса с помощью ссылки на ресурс • mc_class_set Настройка атрибутов класса ресурсов • mc_query_p_select Запрос постоянных атрибутов ресурса путем выбора атрибутов • mc_query_d_select Запрос динамических атрибутов ресурса путем выбора атрибутов

Таблица 176. Записи журнала GR (шаблон записи) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
243 (продолжение)					<ul style="list-style-type: none"> mc_query_p_handle Запрос постоянных атрибутов ресурса с помощью ссылки на ресурс mc_query_d_handle Запрос динамических атрибутов ресурса с помощью ссылки на ресурс mc_class_query_p Запрос постоянных атрибутов класса ресурсов mc_class_query_d Запрос динамических атрибутов класса ресурсов mc_qdef_resource_class Запрос определения класса ресурсов mc_qdef_p_attribute Запрос определения постоянного атрибута mc_qdef_d_attribute Запрос определения динамического атрибута mc_qdef_sd Запрос определения структурированных данных mc_qdef_valid_values Запрос допустимых значений постоянного атрибута mc_qdef_actions Запрос определения действий над ресурсом mc_invoke_action Выполнение действия над ресурсом mc_invoke_class_action Выполнение действия над классом ресурсов
	345	731	CCSID поля 2	Binary (5)	Значение CCSID для поля 2.
	349	735	Длина поля 2	Binary (4)	Длина данных в поле 2.
	351	737	Поле 2	Char (102) ¹	<p>Данные поля 2</p> <p>Для записей типа F данное поле содержит имя выполненной функции.</p> <p>Для записей типа C это поле содержит имя ресурса или класса ресурсов, для которых пользователь попытался выполнить операцию.</p>
	453	839	CCSID поля 3	Binary (5)	Значение CCSID для поля 3.
	457	843	Длина поля 3	Binary (4)	Длина данных в поле 3.

Таблица 176. Записи журнала GR (шаблон записи) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	459	845	Поле 3	Char (102) ¹	<p>Данные поля 3.</p> <p>Для записей типа F данное поле содержит параметры доступа пользователя. Значение в поле задается только в том случае, если выполнялась одна из следующих операций регистрации функции:</p> <p>*REGISTER: Если значение операции равно *REGISTER, это поле содержит права доступа по умолчанию. Имя пользователя будет равно *DEFAULT.</p> <p>*REREGISTER: Если значение операции равно *REGISTER, это поле содержит права доступа по умолчанию. Имя пользователя будет равно *DEFAULT.</p> <p>*CHGUSAGE: Если значение операции равно *CHGUSAGE, это поле содержит права доступа пользователя, имя которого указано в поле Имя пользователя.</p> <p>Для записей типа C это поле содержит результат любой проверки прав доступа, которая была выполнена для операции, указанной в поле 1. Ниже приведены возможные значения:</p> <ul style="list-style-type: none"> • *NOAUTHORITYCHECKED: Если указано это значение, то для выполнения операции, указанной в поле 1, идентификация не требуется, либо идентификация не выполнялась по каким-либо другим причинам. • *AUTHORITYPASSED: Это значение указывается в том случае, если у пользователя, заданного в поле Имя пользовательского профайла, есть необходимые права доступа для выполнения операции из поля 1 над ресурсом или классом ресурсов из поля 2. • *AUTHORITYNOTPASSED: Это значение указывается в том случае, если у пользователя, заданного в поле Имя пользовательского профайла, нет необходимых прав доступа для выполнения операции из поля 1 над ресурсом или классом ресурсов из поля 2.
	561	947	CCSID поля 4	Binary (5)	Значение CCSID для поля 4.
	565	951	Длина поля 4	Binary (4)	Длина данных в поле 4.

Таблица 176. Записи журнала GR (шаблон записи) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	567	953	Поле 4	Char (102) ¹	Данные поля 4. Для записей типа F данное поле содержит разрешающее значение *ALLOBJ для функции. Значение в поле задается только в том случае, если выполнялась одна из следующих операций регистрации функции: *REGISTER *REREGISTER
¹ Это поле переменной длины. Длина поля указывается в первых двух байтах.					

Записи журнала GS (предоставить дескриптор)

В этой таблице представлен формат записей журнала GS (предоставить дескриптор).

Таблица 177. Записи журнала GS (предоставить дескриптор). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. G Предоставить дескриптор Ч Полученный дескриптор U Не удалось применить дескриптор
157	225	611	Имя задания	Char(10)	Имя задания.
167	235	621	Имя польз.	Char(10)	Имя пользователя.
177	245	631	Номер задания	Zoned (6,0)	Номер задания.
183	251	637	Имя пользовательского профайла	Char (10)	Имя пользовательского профайла.
	261	647	JUID	Char (10)	Идентификатор пользователя, связанный с целевым заданием. (Это значение задается только для записей контроля подтипа G.)

Записи журнала IM (монитор вторжений)

В этой таблице представлен формат записей журнала IM (монитор вторжений).

Таблица 178. Записи журнала IM (монитор вторжений). Файл описания полей QASYIMJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		1			Поля заголовка, общие для записей всех типов.
		610	Тип записи	Char(1)	Тип записи. P Обнаружено событие потенциального вторжения
		611	Время события	TIMESTAMP	Время обнаружения события, в формате системного времени SAA.
		637	Идентификатор точки обнаружения	Char(4)	Уникальный идентификатор обрабатывающей единицы, обнаружившей событие вторжения. Это поле предназначено для обслуживающего персонала.
		641	Семейство локальных адресов	Char(1)	Семейство локальных IP-адресов, связанное с обнаруженным событием.
		642	Локальный порт	Zone(5,0)	Локальный порт, связанный с обнаруженным событием.
		647	Локальный IP-адрес	Char(46)	Локальный IP-адрес, связанный с обнаруженным событием.
		693	Семейство удаленных адресов	Char(1)	Семейство удаленных адресов, связанное с обнаруженным событием.
		694	Удаленный порт	Zoned(5,0)	Удаленный порт, связанный с обнаруженным событием.
		699	Удаленный IP-адрес	Char(46)	Удаленный IP-адрес, связанный с обнаруженным событием.

Таблица 178. Записи журнала IM (монитор вторжений) (продолжение). Файл описания полей QASYIMJE/J4/J5

Смещ.			Поле	Отформатированно	Описание
JE	J4	J5			
		745	Идентификатор типа теста	Char(6)	<p>Идентификатор типа теста, использованного для обнаружения потенциального вторжения. Возможны следующие значения:</p> <p>ATTACK Событие обнаружено действием атаки</p> <p>TR-TCP Действие контроля потока обнаружило событие по TCP</p> <p>TR-UDP Действие контроля потока обнаружило событие по UDP</p> <p>SCANE Событие обнаружено действием просмотра событий</p> <p>SCANG Событие обнаружено действием глобального просмотра</p> <p>XATTACK Возможная атака изнутри</p> <p>XTRTCP Исходящий контроль потока обнаружил событие (TCP)</p> <p>XTRUDP Исходящий контроль потока обнаружил событие (UDP)</p> <p>XSCAN Обнаружено событие исходящего сканирования</p>
		751	Коррелятор событий	Char(4)	<p>Уникальный идентификатор данного события вторжения. С помощью этого идентификатора данную контрольную запись можно сопоставлять с другой информацией об обнаружении вторжений.</p>

Таблица 178. Записи журнала IM (монитор вторжений) (продолжение). Файл описания полей QASYIMJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		755	Тип события	Char(8)	Идентификатор типа обнаруженного потенциального вторжения. Возможны следующие значения: ACKSTORM Атака пакетами TCP ACK ADRPOISN Подмена адресов FLOOD Событие лавинной рассылки FRAGGLE Атака типа fraggle ICMPRED Перенаправление ICMP (Протокол управляющих сообщений Internet) IPFRAG Фрагмент IP MALFPKT Неправильно сформированный пакет OUTRAW Исходящий низкоуровневый пакет PERPECH Постоянный эхоповтор PNGDEATH Фатальный пинг RESTOPT Запрещенные опции IP RESTPROT Запрещенный протокол IP SMURF Атака типа smurf
		763	Протокол	Char(3)	Номер протокола
		766	Условие	Char(4)	Номер условия из файла стратегии IDS
		770	Ограничение канала	Char(1)	<ul style="list-style-type: none"> • 0 = неактивно • 1 = активно
		771	Сброшенные пакеты	Zoned(5,0)	Число сброшенных пакетов при ограничении канала
		776	Целевой стек TCP/IP	Char(1)	P Рабочий стек S Служебный стек
		777	Зарезервировано	Char(6)	Пока не используется
		783	Подозр. пакет	Char(1002) ¹	Поле переменной длины, которое может содержать до 1000 начальных байтов пакета IP, связанного с обнаруженным событием. Это поле содержит двоичные данные и должно рассматриваться как поле с CCSID 65 535.

Таблица 178. Записи журнала IM (монитор вторжений) (продолжение). Файл описания полей QASYIMJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
¹ Это поле переменной длины. Информация подозрительного пакета указывается в первых двух байтах.					

Записи журнала IP (обмен данными между процессами)

В этой таблице представлен формат записей журнала IP (обмен данными между процессами).

Таблица 179. Записи журнала IP (обмен данными между процессами). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение принадлежности и/или прав доступа C Создание D Удаление F Отсутствие необходимых прав доступа G Получение M Подключение общей памяти Z Закрытие семафора или отключение общей памяти в обычном режиме
157	225	611	Тип IPC	Char(1)	Тип IPC M Общая память Net Обычный семафор Q Очередь сообщений S Семафор
158	226	612	Ссылка на IPC	Binary(5)	ИД ссылки на IPC
162	230	616	Новый владелец	Char(10)	Новый владелец объекта IPC
172	240	626	Прежний владелец	Char(10)	Прежний владелец объекта IPC
182	250	636	Права доступа владельца	Char(3)	Права доступа владельца к объекту IPC *R чтение *W запись *RW чтение и запись

Таблица 179. Записи журнала IP (обмен данными между процессами) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
185	253	639	Новая группа	Char(10)	Группа, связанная с объектом IPC
195	263	649	Прежняя группа	Char(10)	Предыдущая группа, связанная с объектом IPC
205	273	659	Права доступа группы	Char(3)	Права доступа группы к объекту IPC *R чтение *W запись *RW чтение и запись
208	276	662	Общие права доступа	Char(3)	Общие права доступа к объекту IPC *R чтение *W запись *RW чтение и запись
211	279	665	CCSID имени семафора	Binary(5)	CCSID, связанный с именем семафора.
216	283	669	Длина имени семафора	Binary(4)	Длина имени семафора.
218	285	671	Имя семафора	Char(2050)	Имя семафора. Прим.: Это поле переменной длины. Первые два символа задают длину имени семафора.

Записи журнала IR (действия правил обработки пакетов IP)

В этой таблице представлен формат записей журнала IR (действия правил обработки пакетов IP).

Таблица 180. Записи журнала IR (действия правил обработки пакетов IP). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.
	224	610	Тип записи	Char(1)	Тип записи. L Правила IP загружены из файла. Нет Выгружены правила обработки пакетов IP для защищенного соединения IP P Загружены правила обработки пакетов IP для защищенного соединения IP Ч Правила IP прочитаны и скопированы в файл. U Правила IP выгружены (удалены).

Таблица 180. Записи журнала IP (действия правил обработки пакетов IP) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
	225	611	Имя файла	Char(10)	Имя файла QSYS, с помощью которого выполнялась загрузка и получение правил обработки пакетов IP. Значение в этом поле будет задано только в том случае, если файл располагается в файловой системе QSYS.
	235	621	Библиотека файла	Char(10)	Имя библиотеки файла QSYS.
	245	631	Зарезерв.	Char(18)	
	263	649	Длина имени файла	Binary (4)	Длина имени файла.
	265	651	CCSID имени файла ¹	Binary (5)	CCSID, связанный с именем файла.
	269	655	ИД страны или региона для файла ¹	Char(2)	ИД страны или региона, связанный с именем файла.
	271	657	ИД языка для файла ¹	Char(3)	ИД языка, связанный с именем файла.
	274	660	Зарезерв.	Char(3)	
	277	663	ИД родительского каталога ²	Char(16)	ИД файла, связанный с родительским каталогом.
	293	679	ИД файла объекта ^{1,2}	Char(16)	ИД файла.
	309	695	Имя файла ¹	Char(512)	Имя файла.
	821	1207	Номер соединения	Char(40)	Имя соединения.
	861	1247	ИД файла объекта	Char(16)	ИД файла объекта.
	877	1263	Имя ASP	Char(10)	Имя ASP.
	887	1273	Номер ASP ⁵	Char(5)	Номер ASP.
	892	1278	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	896	1282	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	898	1284	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	901	1287	Длина пути	Binary(4)	Длина имени пути.

Таблица 180. Записи журнала IP (действия правил обработки пакетов IP) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	903	1289	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	904	1290	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	920	1306	Путь ⁴	Char(5002)	Путь к объекту.
1	Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.				
2	Если первый разряд ИД равен 1, а остальные - нулю, значит ИД не задан.				
3	Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.				
4	Это поле переменной длины. Длина поля указывается в первых двух байтах.				
5	Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.				

Записи журнала IS (управление защитой в Internet)

В этой таблице представлен формат записей журнала IS (управление защитой в Internet).

Таблица 181. Записи журнала IS (управление защитой в Internet). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596.
	224	610	Тип записи	Char(1)	Тип записи. A Сбой (данный тип более не применяется) C Обычный (данный тип более не применяется) U Мобильный пользователь (данный тип более не применяется) 1 Согласование SA на первом этапе IKE 2 Согласование SA на втором этапе IKE

Таблица 181. Записи журнала IS (управление защитой в Internet) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	225	611	Локальный IP-адрес ¹	Char(15)	Локальный IP-адрес.
	240	626	Порт локального клиента	Char(5)	Порт локального клиента.
	245	631	Удаленный IP-адрес ¹	Char(15)	Удаленный IP-адрес.
	260	646	Порт удаленного клиента	Char (5)	Порт удаленного клиента (значение применяется только на этапе 2).
	265	651	Семейство локальных IP-адресов	Char(1)	Семейство локальных IP-адресов 4 IPv4 6 IPv6
		652	Локальный IP-адрес	Char (46)	Локальный IP-адрес
		698	Семейство удаленных IP-адресов	Char (1)	Семейство удаленных IP-адресов 4 IPv4 6 IPv6
		699	Удаленный IP-адрес	Char (46)	Удаленный IP-адрес
		745	Зарезервировано	Char (162)	Зарезервировано
	521	907	Код результата	Char(4)	Результат согласования: 0 Успешное 1–30 Ошибки протокола (описаны в документе ISAKMP RFC2408, который можно найти на Web-сайте http://www.ietf.org) 82xx Ошибки Диспетчера ключей VPN i5/OS
	525	911	CCSID	Bin(5)	Идентификатор набора символов для следующих полей: • Локальный ИД • ИД локального клиента • Удаленный ИД • ИД удаленного клиента
	529	915	Локальный ИД	Char(256)	Локальный идентификатор IKE

Таблица 181. Записи журнала IS (управление защитой в Internet) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	785	1171	Тип ИД локального клиента	Char(2)	Тип ИД клиента (применяется на этапе 2): 1 Адрес IPv4 2 Полное имя хоста 3 Пользовательское полное имя хоста 4 Подсеть IPv4 5 Адрес IPv6 6 Подсеть IPv6 7 Диапазон адресов IPv4 8 Диапазон адресов IPv6 9 Отличительное имя 11 Идентификатор ключа
	787	1173	ИД локального клиента	Char(256)	ИД локального клиента (применяется на этапе 2)
	1043	1429	Протокол локального клиента	Char(4)	Протокол локального клиента (применяется на этапе 2)
	1047	1433	Удаленный ИД	Char(256)	Удаленный идентификатор IKE
	1303	1689	Тип ИД удаленного клиента	Char(2)	Тип ИД клиента (применяется на этапе 2): 1 Адрес IPv4 2 Полное имя хоста 3 Пользовательское полное имя хоста 4 Подсеть IPv4 5 Адрес IPv6 6 Подсеть IPv6 7 Диапазон адресов IPv4 8 Диапазон адресов IPv6 9 Отличительное имя 11 Идентификатор ключа
	1305	1691	ИД удаленного клиента	Char(256)	ИД удаленного клиента (применяется на этапе 2).
	1561	1947	Протокол удаленного клиента	Char(4)	Протокол удаленного клиента (применяется на этапе 2)
¹ В этих полях разрешено указывать только адреса IPv4.					

Записи журнала JD (изменение описания задания)

В этой таблице представлен формат записей журнала JD (изменение описания задания).

Таблица 182. Записи журнала JD (изменение описания задания). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Пользовательский профайл из параметра USER описания задания
157	225	611	Описание задания	Char(10)	Имя описания задания, для которого был изменен параметр USER.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Тип команды	Char(3)	Тип указанной команды. CHG Команда Изменить описание задания (CHGJOB). CRT Команда Создать описание задания (CRTJOB).
188	256	642	Прежний пользователь	Char(10)	Имя пользовательского профайла, которое было указано в параметре USER до изменения описания задания.
198	266	652	Новый пользователь	Char(10)	Имя пользовательского профайла, которое было указано в параметре USER при изменении описания задания.
		662	Имя ASP	Char(10)	Имя ASP библиотеки JOB
		672	Номер ASP	Char(5)	Номер ASP библиотеки JOB

Записи журнала JS (изменение задания)

В этой таблице представлен формат записей журнала JS (изменение задания).

Таблица 183. Записи журнала JS (изменение задания). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	<p>Тип записи.</p> <p>A Команда ENDJOBABN</p> <p>B Передача на выполнение</p> <p>C Изменение</p> <p>E Завершение</p> <p>H Блокировка</p> <p>I Отключение</p> <p>J Текущее задание пытается прервать другое задание</p> <p>K Текущее задание вскоре будет прервано</p> <p>L Прерывание текущего задания выполнено</p> <p>M Изменение профайла пользователя или группы</p> <p>Нет Команда ENDJOB</p> <p>P Подключение предварительного задания или пакетного немедленного задания</p> <p>Q Изменение атрибутов запроса</p> <p>Ч Разблокирование</p> <p>S Запуск</p> <p>T Изменение профайла пользователя или группы с помощью одноразового разрешения.</p> <p>U CHGUSRTRC</p> <p>V Смена виртуального устройства с помощью API QWSACCD5.</p>

Таблица 183. Записи журнала JS (изменение задания) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
157	225	611	Тип задания	Char(1)	Тип задания. A Автоматическое B Пакетное I Интерактивное M Монитор подсистемы Ч Программа чтения S Для системы W Программа записи X SCPF
158	226	612	Подтип задания	Char(1)	Подтип задания. ', ' Подтип не задан D Пакетное немедленное E Запрос на запуск процедуры J Предварительное P Печать драйвера устройства Q Запрос T MRT U Пользователь альтернативного буфера
159	227	613	Имя задания	Char(10)	Первый компонент полного имени задания, для которого выполняется действие
169	237	623	Имя пользователя задания	Char(10)	Второй компонент полного имени задания, для которого выполняется действие
179	247	633	Номер задания	Char(6)	Третий компонент полного имени задания, для которого выполняется действие
185	253	639	Имя устройства	Char(10)	Имя устройства
195	263	649	Действующий польз. профайл ²	Char(10)	Имя действующего пользовательского профайла нити
205	273	659	Имя описания задания	Char(10)	Имя описания задания
215	283	669	Библиотека описания задания	Char(10)	Имя библиотеки описания задания
225	293	679	Имя очереди заданий	Char(10)	Имя очереди данного задания
235	303	689	Библиотека очереди заданий	Char(10)	Имя библиотеки очереди заданий
245	313	699	Имя очереди вывода	Char(10)	Имя очереди вывода задания
255	323	709	Библиотека очереди вывода	Char(10)	Имя библиотеки очереди вывода

Таблица 183. Записи журнала JS (изменение задания) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
265	333	719	Принтер	Char(10)	Имя принтера задания
275	343	729	Список библиотек ²	Char(430)	Список библиотек задания
705	773	1159	Имя действующего профайла группы ²	Char(10)	Имя действующего профайла группы для нити
715	783	1169	Доп. профайлы групп ²	Char(150)	Имена дополнительных профайлов групп нити.
	933	1319	Описание JUID	Char(1)	Описывает значение поля JUID: ' ' Поле JUID содержит значение переменной JOB. C Был вызван API очистки JUID. Поле JUID содержит новое значение. S Был вызван API настройки значения JUID. Поле JUID содержит новое значение.
	934	1320	Поле JUID	Char(10)	Содержит значение JUID
	944	1330	Фактический польз. профайл	Char(10)	Имя фактического пользовательского профайла нити.
	954	1340	Сохраненный польз. профайл	Char(10)	Имя сохраненного пользовательского профайла нити.
	964	1350	Фактический профайл группы	Char(10)	Имя фактического профайла группы для нити.
	974	1360	Сохраненный профайл группы	Char(10)	Имя сохраненного профайла группы для нити.
	984	1370	Фактический пользователь изменен ³	Char(1)	Указывает, изменен ли фактический пользовательский профайл. Д Да Нет Нет
	985	1371	Действующее имя пользователя изменено ³	Char(1)	Указывает, изменен ли действующий пользовательский профайл. Д Да Нет Нет
	986	1372	Сохраненное имя пользователя изменено ³	Char(1)	Указывает, изменен ли сохраненный пользовательский профайл Д Да Нет Нет
	987	1373	Фактическая группа изменена ³	Char(1)	Указывает, был ли изменен фактический профайл группы. Д Да Нет Нет

Таблица 183. Записи журнала JS (изменение задания) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	988	1374	Действующая группа изменена ³	Char(1)	Указывает, был ли изменен действующий профайл группы Д Да Нет Нет
	989	1375	Сохраненная группа изменена ³	Char(1)	Указывает, был ли изменен сохраненный профайл группы. Д Да Нет Нет
	990	1376	Доп. группы изменены ³	Char(1)	Указывает, были ли изменены профайлы дополнительных групп. Д Да Нет Нет
	991	1377	Количество библиотек в списке ⁴	Bin(4)	Количество библиотек в поле расширения списка библиотек (смещение 993).
	993	1379	Расширение списка библиотек ^{4,5}	Char(2252)	Расширение списка библиотек задания.
		3631	Группа ASP библиотеки	Char(10)	Группа ASP библиотеки
		3641	Имя ASP	Char(10)	Имя ASP библиотеки JOBQ
		3651	Номер ASP	Char(5)	Номер ASP библиотеки JOBQ
		3656	Имя часового пояса	Char(10)	Описательное имя часового пояса
		3666	Имя задания выхода	Char(10)	Имя задания, прервавшего текущее задание или прерванного текущим заданием
		3676	Пользователь задания выхода	Char(10)	Пользователь задания, прервавшего текущее задание или прерванного текущим заданием
		3686	Номер задания выхода ^{6,7}	Char(6)	Номер задания, прервавшего текущее задание или прерванного текущим заданием
		3692	Имя программы выхода ⁶	Char(10)	Программа выхода, примененная для прерывания задания
		3702	Библиотека программы выхода ⁶	Char(10)	Имя библиотеки программы выхода, примененной для прерывания задания
		3712	Имя ASP библиотеки JOBQ	Char(10)	Имя ASP библиотеки JOBQ
		3722	Номер ASP библиотеки JOBQ	Char(5)	Номер ASP библиотеки JOBQ

Таблица 183. Записи журнала JS (изменение задания) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
1					Если задание находится в очереди заданий и еще не запускалось, значение в этом поле указано не будет.
2					Если запись контроля JS была создана, когда одно задание выполняло действия над другим заданием, то это поле содержит данные о начальной нити того задания, над которым выполнялись действия. В остальных случаях это поле содержит данные о нити, выполнившей операцию.
3					Это поле задается только для записей M и T (смещение 610).
4					Это поле применяется только в том случае, если весь список библиотек не помещается в поле со смещением 729.
5					Это поле переменной длины. Длина данных поля указывается в первых двух байтах.
6					Это поле задается только для записей J, K и L (смещение 610).
7					Если тип записи равен J, то это поле содержит информацию о задании, которое будет прервано. Если тип записи равен K или L, то это поле содержит информацию о задании, запросившем прерывание текущего задания.

Записи журнала KF (файл набора ключей)

В этой таблице представлен формат записей журнала KF (файл набора ключей).

Таблица 184. Записи журнала KF (файл набора ключей). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.
	224	610	Тип записи	Char(1)	Тип записи. C Операция с сертификатом K Операция с файлом набора ключей P Неверный пароль T Операция с надежным базовым сертификатом
	225	611	Операция с сертификатом	Char(3)	Тип действия ⁴ . ADK Добавление сертификата с частным ключом ADD Добавление сертификата REQ Отправка запроса на получение сертификата SGN Создание подписи сертификата

Таблица 184. Записи журнала KF (файл набора ключей) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
	228	614	Операция с набором ключей	Char(3)	Тип действия ⁵ . ADD Добавление пары в набор ключей DFT Выбор пары ключей из набора в качестве ключей по умолчанию EXP Экспорт пары ключей из набора IMP Импорт пары ключей в набор LST Просмотр меток пар ключей из файла набора PWD Изменение пароля файла набора ключей RMV Удаление пары ключей из набора INF Получение сведений о паре ключей из набора 2DB Преобразование файла набора ключей в файл базы данных ключей 2YR Преобразование файла базы данных ключей в файл набора ключей
	231	617	Операция с надежным базовым сертификатом	Char(3)	Тип действия ⁶ . TRS Выбор пары из набора ключей для применения в качестве надежного базового сертификата RMV Удаление сведений о надежном базовом сертификате LST Просмотр списка надежных базовых сертификатов
	234	620	Зарезерв.	Char(18)	
	252	638	Длина имени объекта	Binary(4)	Длина имени файла набора ключей.
	254	640	CCSID имени объекта	Binary(5)	Идентификатор набора символов, связанный с именем файла набора ключей.
	258	644	ИД страны или региона для имени объекта	Char(2)	ИД страны или региона, связанный с именем файла набора ключей.
	260	646	ИД языка для имени объекта	Char(3)	ИД языка, связанный с именем файла набора ключей.
	263	649	Зарезерв.	Char(3)	
	266	652	ИД родительского каталога	Char(16)	ИД файла, связанный с родительским каталогом набора ключей.
	282	668	ИД файла объекта	Char(16)	Имя файла каталога набора ключей.
	298	684	Имя объекта	Char(512)	Имя файла набора ключей.
	810	1196	Зарезерв.	Char(18)	

Таблица 184. Записи журнала KF (файл набора ключей) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	828	1214	Длина имени объекта	Binary(4)	Длина имени исходного или целевого файла.
	830	1216	CCSID имени объекта	Binary(5)	Идентификатор набора символов, связанный с именем исходного или целевого файла.
	834	1220	ИД страны или региона для имени объекта	Char(2)	ИД страны или региона, связанный с именем исходного или целевого файла.
	836	1222	ИД языка для имени объекта	Char(3)	ИД языка, связанный с именем исходного или целевого файла.
	839	1225	Зарезерв.	Char(3)	
	842	1228	ИД родительского каталога	Char(16)	ИД файла, связанный с родительским каталогом исходного или целевого файла.
	858	1244	ИД файла объекта	Char(16)	ИД исходного или целевого каталога.
	874	1260	Имя объекта	Char(512)	Имя исходного или целевого объекта.
	1386	1772	Длина метки сертификата	Binary(4)	Длина метки сертификата.
	1388	1774	Метка сертификата ¹	Char(1026)	Метка сертификата.
	2414	2800	ИД файла объекта	Char(16)	ИД файла набора ключей.
	2430	2816	Имя ASP	Char(10)	Имя ASP.
	2440	2826	Номер ASP	Char(5)	Номер ASP.
	2445	2831	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	2449	2835	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	2451	2837	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	2454	2840	Длина пути	Binary(4)	Длина имени пути.
	2456	2842	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя файла набора ключей. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	2457	2843	Отн. ИД каталога ²	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ²

Таблица 184. Записи журнала KF (файл набора ключей) (продолжение). Файл описания полей QASYCYJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	2473	2859	Полный путь ¹	Char(5002)	Полный путь к файлу набора ключей.
	7475	7861	ИД файла объекта	Char(16)	ИД целевого или исходного файла.
	7491	7877	Имя ASP	Char(10)	Имя ASP исходного или целевого файла
	7501	7887	Номер ASP	Char(5)	Номер ASP исходного или целевого файла
	7506	7892	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	7510	7896	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	7512	7898	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	7515	7901	Длина пути	Binary(4)	Длина имени пути.
	7517	7903	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя исходного или целевого файла. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	7518	7904	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ²
	7534	7920	Полный путь ¹	Char(5002)	Полный путь к исходному или целевому файлу.
¹	Это поле переменной длины. Длина пути указывается в первых двух байтах.				
²	Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.				
³	Если индикатор полного имени (смещение 7517) равен N, данное поле содержит относительный ИД файла, входящий в состав полного пути (смещение 7534). Если индикатор полного пути равен Y, то это поле содержит значение размером 16 байт, состоящее из шестнадцатеричных нулей.				
⁴	Данное поле содержит значение только для операций с сертификатами.				
⁵	Данное поле содержит значение только для операций с файлами набора ключей.				
⁶	Данное поле содержит значение только для операций с надежным базовым сертификатом.				

Записи журнала LD (создание и удаление ссылок, поиск в каталоге)

В этой таблице представлен формат записей журнала LD (создание и удаление ссылок, поиск в каталоге).

Таблица 185. Записи журнала LD (создание и удаление ссылок, поиск в каталоге). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. L Создание связи с каталогом U Удаление связи с каталогом K Поиск в каталоге
157			(Зарезерв.)	Char(20)	
	225	611	(Зарезерв.)	Char(18)	
	243	629	Длина имени объекта ¹	Binary (4)	Длина имени объекта.
177	245	631	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
181	249	635	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
183	251	637	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
186	254	640	(Зарезерв.)	Char(3)	
189	257	643	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
205	273	659	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
221	289	675	Имя объекта ¹	Char(512)	Имя объекта.
	801	1187	ИД файла объекта	Char(16)	ИД файла объекта.
	817	1203	Имя ASP	Char(10)	Имя ASP.
	827	1213	Номер ASP	Char(5)	Номер ASP.
	832	1218	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	836	1222	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	838	1224	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	841	1227	Длина пути	Binary(4)	Длина имени пути.

Таблица 185. Записи журнала LD (создание и удаление ссылок, поиск в каталоге) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	843	1229	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	844	1230	Отн. ИД каталога ¹	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ¹
	860	1246	Путь ²	Char(5002)	Путь к объекту.
¹ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка. ² Это поле переменной длины. Длина пути указывается в первых двух байтах.					

Записи журнала ML (действия с почтой)

В этой таблице представлен формат записей журнала ML (действия с почтой).

Таблица 186. Записи журнала ML (действия с почтой). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. О Открыт протокол почты
157	225	611	Пользовательский профайл	Char(10)	Имя пользовательского профайла.
167	235	621	ИД пользователя	Char(8)	Идентификатор пользователя
175	243	629	Адрес	Char(8)	Адрес пользователя

Записи журнала NA (изменение атрибута)

В этой таблице представлен формат записей журнала NA (изменение атрибута).

Таблица 187. Записи журнала NA (изменение атрибута). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение сетевого атрибута. T Изменение атрибута TCP/IP.
157	225	611	Атрибут	Char(10)	Имя атрибута.
167	235	621	Новое значение атрибута	Char(250)	Значение атрибута после изменения.
417	485	871	Прежнее значение атрибута	Char(250)	Значение атрибута до изменения.

Записи журнала ND (фильтр поиска в каталоге APPN)

В этой таблице представлен формат записей журнала ND (фильтр поиска в каталоге APPN).

Таблица 188. Записи журнала ND (фильтр поиска в каталоге APPN). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Нарушение фильтра поиска в каталоге
157	225	611	Имя выбранной управляющей точки	Char(8)	Имя выбранной управляющей точки
165	233	619	NETID выбранной управляющей точки.	Char(8)	NETID выбранной управляющей точки.

Таблица 188. Записи журнала ND (фильтр поиска в каталоге APPN) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
173	241	627	Имя расположения выбранной управляющей точки	Char(8)	Имя расположения выбранной управляющей точки.
181	249	635	NETID расположения выбранной управляющей точки	Char(8)	NETID расположения выбранной управляющей точки.
189	257	643	Имя расположения партнера	Char(8)	Имя расположения партнера.
197	265	651	NETID расположения партнера	Char(8)	NETID расположения партнера.
205	273	659	Сеанс приема	Char(1)	Сеанс приема. Д Данный сеанс является сеансом приема Нет Данный сеанс не является сеансом приема
206	274	660	Сеанс отправки	Char(1)	Сеанс отправки. Д Данный сеанс является сеансом отправки Нет Данный сеанс не является сеансом отправки

Дополнительная информация о фильтре поиска в каталоге APPN и конечных точках APPN приведена в разделе Защита системы в среде APPN и HPR.

Записи журнала NE (фильтр конечной точки APPN)

В этой таблице представлен формат записей журнала NE (фильтр конечной точки APPN).

Таблица 189. Записи журнала NE (фильтр конечной точки APPN). Файл описания полей QASYNEJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 189. Записи журнала NE (фильтр конечной точки APPN) (продолжение). Файл описания полей QASYNEJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Тип записи	Char(1)	Тип записи. A Нарушение фильтра конечной точки
157	225	611	Имя локального расположения	Char(8)	Имя локального расположения.
165	233	619	Имя удаленного расположения	Char(8)	Имя удаленного расположения.
173	241	627	Удаленный NETID	Char(8)	Удаленный NETID.
181	249	635	Сеанс приема	Char(1)	Сеанс приема. Д Данный сеанс является сеансом приема Нет Данный сеанс не является сеансом приема
182	250	636	Сеанс отправки	Char(1)	Сеанс отправки. Д Данный сеанс является сеансом отправки Нет Данный сеанс не является сеансом отправки

Дополнительная информация о фильтре поиска в каталоге APPN и конечных точках APPN приведена в разделе Защита системы в среде APPN и HPR.

Записи журнала OM (изменение параметров управления объектами)

В этой таблице представлен формат записей журнала OM (изменение параметров управления объектами).

Таблица 190. Записи журнала OM (изменение параметров управления объектами). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. M Объект перемещен в другую библиотеку. Ч Объект переименован.

Таблица 190. Записи журнала OM (изменение параметров управления объектами) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
157	225	611	Прежнее имя объекта	Char(10)	Прежнее имя объекта.
167	235	621	Прежнее имя библиотеки	Char(10)	Имя библиотеки, в которой находится прежний объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Новое имя объекта	Char(10)	Новое имя объекта.
195	263	649	Новое имя библиотеки	Char(10)	Имя библиотеки, в которую был перемещен объект.
205	273		(Зарезерв.)	Char(20)	
		659	Атрибут объекта	Char(10)	Атрибут объекта.
		669	(Зарезерв.)	Char(10)	
225	293	679	Польз. Office	Char(10)	Имя пользователя Office.
235	303	689	Прежнее имя папки или документа	Char(12)	Прежнее имя папки или документа.
247	315	701	(Зарезерв.)	Char(8)	
255	323	709	Полное имя прежней папки	Char(63)	Полное имя прежней папки.
318	386	772	Новое имя папки или документа	Char(12)	Новое имя папки или документа.
330	398	784	(Зарезерв.)	Char(8)	
338	406	792	Полное имя новой папки	Char(63)	Полное имя новой папки.
401	469	855	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
411			(Зарезерв.)	Char(20)	
	479	865	(Зарезерв.)	Char(18)	
	497	883	Длина имени объекта	Binary(4)	Длина поля прежнего имени объекта.
431	499	885	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
435	503	889	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
437	505	891	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
440	508	894	(Зарезерв.)	Char(3)	

Таблица 190. Записи журнала ОМ (изменение параметров управления объектами) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
443	511	897	ИД прежнего родительского каталога ^{1,2}	Char(16)	ИД файла, связанный с прежним родительским каталогом.
459	527	913	Прежний ИД файла объекта ^{1,2}	Char(16)	Прежний ИД файла объекта.
475	543	929	Прежнее имя объекта ¹	Char(512)	Прежнее имя объекта.
987	1055	1441	ИД нового родительского каталога ^{1,2}	Char(16)	ИД нового родительского каталога.
1003	1071	1457	Новое имя объекта ^{1,2,6}	Char(512)	Новое имя объекта.
	1583	1969	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
	1599	1985	Имя ASP ⁷	Char(10)	Имя ASP.
	1609	1995	Номер ASP ⁷	Char(5)	Номер ASP.
	1614	2000	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	1618	2004	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	1620	2006	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	1623	2009	Длина пути	Binary(4)	Длина имени пути.
	1625	2011	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	1626	2012	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1642	2028	Полный путь ⁵	Char(5002)	Прежнее полное имя объекта.
	6644	7030	ИД файла объекта	Char(16)	ИД файла объекта.
	6660	7046	Имя ASP ⁸	Char(10)	Имя ASP.
	6670	7056	Номер ASP ⁸	Char(5)	Номер ASP.
	6675	7061	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.

Таблица 190. Записи журнала OM (изменение параметров управления объектами) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	6679	7065	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	6681	7067	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	6684	7070	Длина пути	Binary(4)	Длина имени пути.
	6686	7072	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	6687	7073	Отн. ИД каталога ⁴	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	6703	7089	Полный путь ⁵	Char(5002)	Новое полное имя объекта.

- ¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.
- ² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.
- ³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.
- ⁴ Если индикатор полного имени (смещение 6686) равен N, данное поле содержит относительный ИД файла, входящий в состав полного пути (смещение 6703). Если индикатор полного пути равен Y, то это поле содержит значение размером 16 байт, состоящее из шестнадцатеричных нулей.
- ⁵ Это поле переменной длины. Длина пути указывается в первых двух байтах.
- ⁶ Длина этого значения не указывается. Строка дополняется нулями до 512 символов.
- ⁷ Если прежний объект располагался в какой-либо библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.
- ⁸ Если новый объект расположен в какой-либо библиотеке, то информация об ASP относится к этой библиотеке. В противном случае информация об ASP относится к самому объекту.

Записи журнала OR (восстановление объекта)

В этой таблице представлен формат записей журнала OR (восстановление объекта).

Таблица 191. Записи журнала OR (восстановление объекта). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594; “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. Нет В системе восстановлен новый объект. Е В системе был восстановлен существующий объект.
157	225	611	Имя восст. объекта	Char(10)	Имя восстановленного объекта.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки восстановленного объекта.
177	245	631	Тип объекта.	Char(8)	Тип объекта.
185	253	639	Имя объекта сохранения	Char(10)	Имя объекта сохранения.
195	263	649	Имя библиотеки сохранения	Char(10)	Имя библиотеки, из которой был сохранен объект.
205	273	659	Состояние программы ¹	Char(1)	I Восстановлена программа режима наследования. Д Восстановлена программа режима системы. Нет Восстановлена программа режима пользователя.
206	274	660	Системная команда ²	Char(1)	Д Восстановлена системная команда. Нет Восстановлена команда режима пользователя.
207			(Зарезерв.)	Char(18)	
	275	661	Режим SETUID	Char(1)	Индикатор режима SETUID. Д Для восстановленного объекта установлен бит режима SETUID. Нет Для восстановленного объекта не установлен бит режима SETUID.
	276	662	Режим SETGID	Char(1)	Индикатор режима SETGID. Д Для восстановленного объекта установлен бит режима SETGID. Нет Для восстановленного объекта не установлен бит режима SETGID.

Таблица 191. Записи журнала OR (восстановление объекта) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	277	663	Состояние подписи	Char(1)	Состояние подписи восстановленного объекта. B Формат подписи отличается от формата i5/OS E Подпись существует, но она не проверена F Подпись не соответствует содержимому объекта I Подпись проигнорирована Нет Объект не допускает создание подписи S Объект содержит верную подпись T Подпись не является надежной U У объекта нет подписи
	278	664	Атрибут просмотра	Char(1)	Если файл являлся объектом интегрированной файловой системы, то это поле содержит одно из следующих значений атрибута просмотра объекта: Д *YES Нет *NO С *CHGONLY Описания этих значений можно просмотреть с помощью команды CHGATR.
	279		(Зарезерв.)	Char(14)	
		665	Атрибут объекта	Char(10)	Атрибут объекта.
		675	(Зарезерв.)	Char(4)	
225	293	679	Польз. Office	Char(10)	Имя пользователя Office.
235	303	689	Имя восст. DLO	Char(12)	Имя восстановленного объекта в библиотеке документов.
247	315	701	(Зарезерв.)	Char(8)	
255	323	709	Полное имя папки восст.	Char(63)	Папка, в которой был восстановлен объект DLO.
318	386	772	Имя сохр. DLO	Char(12)	Имя сохраненного объекта библиотеки документов.
330	398	784	(Зарезерв.)	Char(8)	
338	406	792	Полное имя папки сохр.	Char(63)	Папка, в которой располагался сохраненный DLO.
401	469	855	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
411			(Зарезерв.)	Char(20)	
	479		(Зарезерв.)	Char(18)	

Таблица 191. Записи журнала OR (восстановление объекта) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		865	Восстановить частные права доступа	Char(1)	Частные права доступа, которые требуется восстановить (указан параметр PVTAUT(*YES) для команды восстановления) Д Указан параметр PVTAUT(*YES) для команды восстановления Нет Указан параметр PVTAUT(*NO) для команды восстановления
		866	Сохраненные частные права доступа ⁸	Binary(5)	Число сохраненных частных прав доступа
		870	Восстановленные частные права доступа ⁸	Binary(5) ⁸	Число восстановленных частных прав доступа
		874	(Зарезерв.)	Char(9)	
	497	883	Длина имени объекта	Binary (4)	Длина поля Прежнее имя объекта.
431	499	885	CCSID имени объекта ³	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
435	503	889	ИД страны или региона для имени объекта ³	Char(2)	ИД страны или региона, связанный с именем объекта.
437	505	891	ИД языка для имени объекта ³	Char(3)	ИД языка, связанный с именем объекта.
440	508	894	(Зарезерв.)	Char(3)	
443	511	897	ИД родительского файла ^{3,4}	Char(16)	ИД файла, связанный с родительским каталогом.
459	527	913	ИД файла объекта ^{3,4}	Char(16)	ИД файла объекта.
475	543	929	Имя объекта ³	Char(512)	Имя объекта.
	1055	1441	Прежний ИД файла	Char(16)	Прежний ИД файла объекта.
	1071	1457	ИД файла носителя	Char(16)	ИД файла (FID), сохраненный в файле носителя. Прим.: Сохраненный на носителе FID совпадает с FID объекта в исходной системе.
	1087	1473	ИД файла объекта	Char(16)	ИД файла объекта.
	1103	1489	Имя ASP ⁷	Char(10)	Имя ASP.
	1113	1499	Номер ASP ⁷	Char(5)	Номер ASP.
	1118	1504	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.

Таблица 191. Записи журнала OR (восстановление объекта) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1122	1508	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	1124	1510	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	1127	1513	Длина пути	Binary(4)	Длина имени пути.
	1129	1515	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	1130	1516	Отн. ИД каталога ⁵	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ⁵
	1146	1532	Путь ⁶	Char(5002)	Путь к объекту.
1	Значение в этом поле указывается только в том случае, если восстановленный объект - это программа.				
2	Значение в этом поле указывается только в том случае, если восстановленный объект - это команда.				
3	Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.				
4	Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.				
5	Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.				
6	Это поле переменной длины. Длина пути указывается в первых двух байтах.				
7	Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.				
8	Это поле равно нулю, если параметр Восстановить частные права доступа (смещение 865) равен N.				

Записи журнала OW (изменение владельца)

В этой таблице представлен формат записей журнала OW (изменение владельца).

Таблица 192. Записи журнала OW (изменение владельца). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение владельца объекта
157	225	611	Имя объекта	Char(10)	Имя объекта.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Прежний владелец	Char(10)	Прежний владелец объекта.
195	263	649	Новый владелец	Char(10)	Новый владелец объекта.
205	273	659	(Зарезерв.)	Char(20)	
225	293	679	Польз. Office	Char(10)	Имя пользователя Office.
235	303	689	Имя DLO	Char(12)	Имя объекта библиотеки документов.
247	315	701	(Зарезерв.)	Char(8)	
255	323	709	Полное имя папки	Char(63)	Полное имя папки.
318	386	772	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
328			(Зарезерв.)	Char(20)	
	396	782	(Зарезерв.)	Char(18)	
	414	800	Длина имени объекта	Binary (4)	Длина нового имени объекта.
348	416	802	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
352	420	806	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
354	422	808	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
357	425	811	(Зарезерв.)	Char(3)	
360	428	814	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.

Таблица 192. Записи журнала OW (изменение владельца) (продолжение). Файл описания полей QASYDOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
376	444	830	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
392	460	846	Имя объекта ¹	Char(512)	Имя объекта.
	972	1358	ИД файла объекта	Char(16)	ИД файла объекта.
	988	1374	Имя ASP ⁵	Char(10)	Имя ASP.
	998	1384	Номер ASP ⁵	Char(5)	Номер ASP.
	1003	1389	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	1007	1393	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	1009	1395	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	1012	1398	Длина пути	Binary(4)	Длина имени пути.
	1014	1400	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	1015	1401	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1031	1417	Путь ⁴	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁵ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала O1 (доступ к оптической памяти)

В этой таблице представлен формат записей журнала O1 (доступ к оптической памяти).

Таблица 193. Записи журнала O1 (доступ к оптической памяти). Файл описания полей QASY01JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	R-Чтение U-Обновление D-Удаление C-Создание каталога X-Разблокирование файла
157	225	611	Тип объекта	Char(1)	F-Файл D-Каталог S-Память
158	226	612	Тип доступа	Char(1)	D-Данные файла A-Атрибуты каталога файла R-Операция восстановления S-Операция сохранения
159	227	613	Имя устройства	Char(10)	Имя библиотечного LUD
169	237	623	Имя CSI	Char(8)	Имя дополнительного объекта
177	245	631	Библиотека CSI	Char(10)	Библиотека дополнительного объекта
187	255	641	Имя тома	Char(32)	Имя оптического тома
219	287	673	Имя объекта	Char(256)	Имя оптического каталога/имя файла
		929	Имя ASP	Char(10)	Имя ASP библиотеки CSI
		939	Номер ASP	Char(5)	Номер ASP библиотеки CSI
<p>Примечание: Эта запись применяется для контроля за выполнением следующих действий над оптической памятью:</p> <ul style="list-style-type: none"> • Открытие файла или каталога • Создание каталога • Удаление каталога файлов • Изменение или получение атрибутов • Разблокирование оптического файла 					

Записи журнала O2 (доступ к оптической памяти)

В этой таблице представлен формат записей журнала O2 (доступ к оптической памяти).

Таблица 194. Записи журнала O2 (доступ к оптической памяти). Файл описания полей QASY02JE/J4/J5

Смещ.			Поле	Формат	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594; “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	<p>C-Копирование</p> <p>R-Переименование</p> <p>B-Сохранение каталога или файла</p> <p>S-Сохранение заблокированного файла</p> <p>M-Перемещение файла</p>
157	225	611	Тип объекта	Char(1)	<p>F-Файл</p> <p>D-Каталог</p>
158	226	612	Имя исходного устройства	Char(10)	Имя исходного библиотечного LUD
168	236	622	Имя исходного CSI	Char(8)	Имя исходного дополнительного объекта
176	244	630	Библиотека исходного CSI	Char(10)	Библиотека исходного дополнительного объекта
186	254	640	Имя исходного тома	Char(32)	Имя исходного оптического тома
218	286	672	Имя исходного объекта	Char(256)	Имя исходного оптического каталога/имя файла
474	542	928	Имя целевого устройства	Char(10)	Имя целевого библиотечного LUD
484	552	938	Имя целевого CSI	Char(8)	Имя целевого дополнительного объекта
492	560	946	Библиотека целевого CSI	Char(10)	Библиотека целевого дополнительного объекта
502	570	956	Имя целевого тома	Char(32)	Имя целевого оптического тома
534	602	988	Имя целевого объекта	Char(256)	Имя целевого оптического каталога/имя файла
		1244	Имя ASP	Char(10)	Имя ASP библиотеки исходного CSI
		1254	Номер ASP	Char(5)	Номер ASP библиотеки исходного CSI
		1259	Имя ASP библиотеки целевого CSI	Char(10)	Имя ASP библиотеки целевого CSI

Таблица 194. Записи журнала O2 (доступ к оптической памяти) (продолжение). Файл описания полей QASY02JE/J4/J5

Смещ.			Поле	Формат	Описание
JE	J4	J5			
		1269	Номер ASP библиотеки целевого CSI	Char(5)	Номер ASP библиотеки целевого CSI

Записи журнала O3 (доступ к оптической памяти)

В этой таблице представлен формат записей журнала O3 (доступ к оптической памяти).

Таблица 195. Записи журнала O3 (доступ к оптической памяти). Файл описания полей QASY03JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	A Изменить атрибуты тома B Резервный том C Преобразовать резервный том в основной E Экспорт I Инициализация K Проверить том L Изменить список прав доступа M Импорт Нет Переименование Ч Абсолютное чтение
157	225	611	Имя устройства	Char(10)	Имя библиотечного LUD
167	235	621	Имя CSI	Char(8)	Имя дополнительного объекта
175	243	629	Библиотека CSI	Char(10)	Библиотека дополнительного объекта
185	253	639	Старое имя тома	Char(32)	Старое имя оптического тома
217	285	671	Новое имя тома ¹	Char(32)	Новое имя оптического тома
249	317	703	Старый список прав доступа ²	Char(10)	Старый список прав доступа

Таблица 195. Записи журнала ОЗ (доступ к оптической памяти) (продолжение). Файл описания полей QASYO3JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
259	327	713	Новый список прав доступа ³	Char(10)	Новый список прав доступа
269	337	723	Адрес ⁴	Binary(5)	Начальный блок
273	341	727	Длина ⁴	Binary(5)	Длина считываемых данных
		731	Имя ASP	Char(10)	Имя ASP библиотеки CSI
		741	Номер ASP	Char(5)	Номер ASP библиотеки CSI
<p>¹ Это поле содержит новое имя тома для функций Инициализировать, Переименовать и Преобразовать или имя тома резервной копии для функций резервного копирования. Для функций Импортировать, Экспортировать, Изменить список прав доступа, Изменить атрибуты тома и Прочитать сектор это поле содержит имя тома.</p> <p>² Применяется только для функций Импортировать, Экспортировать и Изменить список прав доступа.</p> <p>³ Применяется только для функции Изменить список прав доступа.</p> <p>⁴ Применяется только для функции Прочитать сектор.</p>					

Записи журнала РА (принятие прав доступа программой)

В этой таблице представлен формат записей журнала РА (принятие прав доступа программой).

Таблица 196. Записи журнала РА (принятие прав доступа программой). Файл описания полей QASYPAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	<p>Тип записи.</p> <p>A Изменить программу так, чтобы она приняла права доступа владельца.</p> <p>J Программа на Java приняла права доступа владельца.</p> <p>M Изменить SETUID, SETGID или индикатор режима ограниченного изменения имен и удаления для объекта.</p>
157	225	611	Имя программы ³	Char(10)	Имя программы.
167	235	621	Библиотека программы ³	Char(10)	Имя библиотеки, в которой расположена программа.
177	245	631	Тип объекта	Char(8)	Тип объекта.

Таблица 196. Записи журнала PA (принятие прав доступа программой) (продолжение). Файл описания полей QASYPAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
185	253	639	Владелец	Char(10)	Имя владельца.
	263	649	Режим ISVTX	Char(1)	Индикатор флага Ограничить изменение имен и удаление (ISVTX). Д Флаг ISVTX включен для объекта. Нет Флаг ISVTX не включен для объекта.
	263	649	Зарезервировано	Char(17)	
	281	667	Длина имени объекта ¹	Binary (4)	Длина имени объекта.
	283	669	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
	287	673	ИД страны или региона для имени объекта	Char(2)	ИД страны или региона, связанный с именем объекта.
	289	675	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
	292	678	Зарезерв.	Char(3)	
	295	681	ИД предка ^{1, 2, 3}	Char(16)	ИД родительского файла.
	311	697	ИД файла объекта ³	Char(16)	ИД файла, связанный с объектом
	327	713	Имя объекта ¹	Char(512)	Имя объекта.
	839	1225	Режим SETUID	Char(1)	Индикатор флага Задать действующий ИД пользователя (SETUID). Д Флаг SETUID включен для объекта. Нет Флаг SETUID выключен для объекта.
	840	1226	Режим SETGID	Char(1)	Индикатор флага Задать действующий ИД группы (SETGID). Д Флаг SETGID включен для объекта. Нет Флаг SETGID выключен для объекта.
	841	1227	Владелец основной группы	Char(10)	Имя владельца основной группы.
	851	1237	ИД файла объекта	Char(16)	ИД файла объекта.
	867	1253	Имя ASP ⁶	Char(10)	Имя ASP.
	877	1263	Номер ASP ⁶	Char(5)	Номер ASP.
	882	1268	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	886	1272	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	888	1274	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	891	1277	Длина пути	Binary(4)	Длина имени пути.

Таблица 196. Записи журнала PA (принятие прав доступа программой) (продолжение). Файл описания полей QASYPAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	893	1279	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	894	1280	Отн. ИД каталога ⁴	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ⁴
	910	1296	Путь ⁵	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если тип записи равен J, то в полях имени программы и имени библиотеки будет указано значение *N. Кроме того, поля ИД родительского файла и ИД файла объекта будут заполнены двоичными нулями.</p> <p>⁴ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁵ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁶ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала PG (изменение основной группы)

В этой таблице представлен формат записей журнала PG (изменение основной группы).

Таблица 197. Записи журнала PG (изменение основной группы). Файл описания полей QASYPGJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменить основную группу.
157	225	611	Имя объекта	Char(10)	Имя объекта.
167	235	621	Библиотека объекта	Char(10)	Имя библиотеки, содержащей объект.

Таблица 197. Записи журнала PG (изменение основной группы) (продолжение). Файл описания полей QASYPGJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Старая основная группа	Char(10)	Предыдущая основная группа объекта. ⁵
195	263	649	Новая основная группа	Char(10)	Новая основная группа объекта.
					Права доступа новой основной группы:
205	273	659	Существование объекта	Char(1)	Д *OBJEXIST
206	274	660	Управление объектом	Char(1)	Д *OBJMGT
207	275	661	Операционные права доступа к объекту	Char(1)	Д *OBJOPR
208	276	662	Изменение объекта	Char(1)	Д *OBJALTER
209	277	663	Обращение к объекту	Char(1)	Д *OBJREF
210	278	664	(Зарезерв.)	Char(10)	
220	288	674	Управление списком прав доступа	Char(1)	Д *AUTLMGT
221	289	675	Права на чтение	Char(1)	Д *READ
222	290	676	Права на добавление	Char(1)	Д *ADD
223	291	677	Права на обновление	Char(1)	Д *UPD
224	292	678	Права на удаление	Char(1)	Д *DLT
225	293	679	Права на выполнение	Char(1)	Д *EXECUTE
226	294	680	(Зарезерв.)	Char(10)	
236	304	690	Исключающие права доступа	Char(1)	Д *EXCLUDE
237	305	691	Аннулирование старой основной группы	Char(1)	Д Аннулировать права доступа старой основной группы. '' Не аннулировать права доступа старой основной группы.
238	306	692	(Зарезерв.)	Char (20)	
258	326	712	Польз. Office	Char(10)	Имя пользователя Office.
268	336	722	Имя DLO	Char(12)	Имя объекта библиотеки документов или папки.
280	348	734	(Зарезерв.)	Char(8)	
288	356	742	Полное имя папки	Char(63)	Полное имя папки.

Таблица 197. Записи журнала PG (изменение основной группы) (продолжение). Файл описания полей QASYPGJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
351	419	805	Польз. Office, работающий от другого имени	Char(10)	Пользователь, работающий от имени другого пользователя.
361			(Зарезерв.)	Char(20)	
	429	815	(Зарезерв.)	Char(18)	
	447	833	Длина имени объекта ¹	Binary (4)	Длина имени объекта.
381	449	835	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
385	453	839	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
387	455	841	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
390	458	844	(Зарезерв.)	Char(3)	
393	461	847	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
409	477	863	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
425	493	879	Имя объекта ¹	Char(512)	Имя объекта.
	1005	1391	ИД файла объекта	Char(16)	ИД файла объекта.
		1407	Имя ASP ⁶	Char(10)	Имя ASP.
		1417	Номер ASP ⁶	Char(5)	Номер ASP.
	1035	1422	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
1	1040	1426	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
1	1042	1428	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
1	1045	1431	Длина пути	Binary(4)	Длина имени пути.
	1047	1433	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	1048	1434	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1064	1450	Путь ⁴	Char(5002)	Путь к объекту.

Таблица 197. Записи журнала PG (изменение основной группы) (продолжение). Файл описания полей QASYPGJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1					Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.
2					Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.
3					Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.
4					Это поле переменной длины. Длина пути указывается в первых двух байтах.
5					Значение *N указывает, что старая основная группа неизвестна.
6					Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.

Записи журнала PO (вывод на принтер)

В этой таблице представлен формат записей журнала PO (вывод на принтер).

Таблица 198. Записи журнала PO (вывод на принтер). Файл описания полей QASYPOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.
156	224	610	Тип вывода	Char(1)	Тип вывода. D Печать без буферизации Ч Отправлен для печати в удаленную систему S Буферный файл
157	225	611	Состояние после печати	Char(1)	D Удалить после печати H Блокировать после печати S Сохранить после печати , , Печать без буферизации
158	226	612	Имя задания	Char(10)	Первый компонент полного имени задания.
168	236	622	Имя пользователя задания	Char(10)	Второй компонент полного имени задания.
178	246	632	Номер задания	Zoned(6,0)	Третий компонент полного имени задания.
184	252	638	Пользовательский профайл	Char(10)	Пользовательский профайл, создавший вывод.

Таблица 198. Записи журнала PO (вывод на принтер) (продолжение). Файл описания полей QASYPOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
194	262	648	Очередь вывода	Char(10)	Очередь вывода, содержащая буферный файл. ¹
204	272	658	Имя библиотеки очереди вывода	Char(10)	Имя библиотеки, содержащей очередь вывода. ¹
214	282	668	Имя устройства	Char(10)	Устройство, на котором был напечатан вывод ² .
224	292	678	Тип устройства	Char(4)	Тип принтера ² .
228	296	682	Модель устройства	Char(4)	Модель принтера ² .
232	300	686	Имя файла устройства	Char(10)	Имя файла устройства, применяемого для доступа к принтеру.
242	310	696	Библиотека файла устройства	Char(10)	Имя библиотеки, содержащей файл устройства.
252	320	706	Имя буферного файла	Char(10)	Имя буферного файла ¹
262	330	716	Короткий номер буферного файла	Char(4)	Номер буферного файла ¹ . Пробел, если номер слишком длинный.
266	334	720	Тип формы	Char(10)	Тип формы буферного файла.
276	344	730	Польз. данные	Char(10)	Пользовательские данные, связанные с буферным файлом ¹ .
286			(Зарезерв.)	Char(20)	
	354	740	Номер буферного файла	Char(6)	Номер буферного файла.
	360	746	Зарезерв. область	Char(14)	
306	374	760	Удаленная система	Char(255)	Имя удаленной системы, которой был отправлен вывод для печати.
561	629	1015	Очередь печати удаленной системы	Char(128)	Имя очереди печати удаленной системы.
	757	1143	Имя системы задания буферного файла	Char (8)	Имя системы, в которой хранится буферный файл.
	765	1151	Дата создания буферного файла	Char (7)	Дата создания буферного файла (ВГГММДД)

Таблица 198. Записи журнала PO (вывод на принтер) (продолжение). Файл описания полей QASYPOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	772	1158	Время создания буферного файла	Char(6)	Время создания буферного файла (ЧЧММСС).
		1164	Имя ASP	Char(10)	Имя ASP библиотеки файла устройства
		1174	Номер ASP	Char(5)	Номер ASP библиотеки файла устройства
		1179	Имя ASP очереди вывода	Char(10)	Имя ASP библиотеки очереди вывода.
		1189	Номер ASP очереди вывода	Char(5)	Номер ASP библиотеки очереди вывода.
		1194	Дата создания буферного файла, UTC	Char(7)	Дата создания буферного файла в UTC. (Совпадает с датой создания буферного файла (смещение 1151), но указывается в UTC).
		1201	Время создания буферного файла, UTC	Char(6)	Время создания буферного файла в UTC. (Совпадает с временем создания буферного файла (смещение 1158), но указывается в UTC)
¹ Это поле пусто, если тип вывода - печать без буферизации. ² Это поле пусто, если тип вывода - удаленная печать.					

Записи журнала PS (смена профайла)

В этой таблице представлен формат записей журнала PS (смена профайла).

Таблица 199. Записи журнала PS (смена профайла). Файл описания полей QASYPSJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 199. Записи журнала PS (смена профайла) (продолжение). Файл описания полей QASYPSJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Тип записи	Char(1)	<p>Тип записи.</p> <p>A Смена профайла во время удаленного входа в систему.</p> <p>E Завершение работы от имени другого пользователя.</p> <p>H Ссылка на профайл, созданная QSYGETPH.</p> <p>I Аннулированы все разрешения</p> <p>M Выдано максимальное число разрешений.</p> <p>P Для пользователя создан маркер профайла.</p> <p>Ч Все маркеры профайла пользователя удалены.</p> <p>S Начало работы от имени другого пользователя</p> <p>V Идентифицирован пользовательский профайл</p>
157	225	611	Пользовательский профайл	Char(10)	Имя пользовательского профайла.
167	235	621	Исходное расположение	Char(8)	Исходное расположение для удаленного входа в систему.
175	243	629	Первоначальный целевой польз. профайл	Char(10)	Первоначальный целевой пользовательский профайл для удаленного входа в систему.
185	253	639	Новый целевой польз. профайл	Char(10)	Новый целевой пользовательский профайл для удаленного входа в систему.
195	263	649	Польз. Office	Char(10)	Пользователь Office, начавший или завершивший работу от имени другого пользователя.
205	273	659	Пользователь, от имени которого выполняется работа	Char(10)	Пользователь, от имени которого работает пользователь Office.
215	283	669	Тип разрешения	Char(1)	<p>Тип созданного разрешения.</p> <p>M Многоразовое разрешение</p> <p>Ч Многоразовое повторно созданное разрешение</p> <p>S Одноразовое разрешение</p>
216	284	670	Тайм-аут разрешения	Binary(4)	Время в секундах, в течение которого действительно разрешение, выданное профайлу

Записи журнала PW (пароль)

В этой таблице представлен формат записей журнала PW (пароль).

Таблица 200. Записи журнала PW (пароль). Файл описания полей QASYPWJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи об ошибке	Char(1)	<p>Тип ошибки</p> <p>A Сбой связывания APPC.</p> <p>C Идентификация пользователя с помощью команды CHKPWD не выполнена.</p> <p>D Неверное имя пользователя сервисных средств.</p> <p>E Неверный пароль пользователя сервисных средств.</p> <p>P Неверный пароль.</p> <p>Q Попытка войти в систему (идентификация пользователя) не удалась, поскольку пользовательский профайл отключен.</p> <p>Ч Попытка войти в систему (идентификация пользователя) не удалась, поскольку срок действия пароля истек. В некоторых механизмах идентификации пользователей эта контрольная запись не выдается. Некоторые механизмы идентификации не проверяют, устарели ли пароли.</p> <p>S Неверный пароль для расшифровки данных SQL.</p> <p>U Неверное имя пользователя.</p> <p>X ИД пользователя сервисных средств заблокирован.</p> <p>Д Неверный ИД пользователя сервисных средств.</p> <p>Z Неверный пароль пользователя сервисных средств.</p>
157	225	611	Имя польз.	Char(10)	Имя пользователя задания или имя пользователя сервисных средств.

Таблица 200. Записи журнала PW (пароль) (продолжение). Файл описания полей QASYPWJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
167	235	621	Имя устройства	Char(40)	Имя обычного устройства или устройства связи, на котором был введен ИД пользователя. Если тип записи равен X, Y или Z, то это поле содержит имя запрошенного сервисного средства.
207	275	661	Имя удаленного расположения	Char(8)	Имя удаленного расположения для связывания APPC.
215	283	669	Имя локального расположения	Char(8)	Имя локального расположения для связывания APPC.
223	291	677	ИД сети	Char(8)	ИД сети для связывания APPC.
		685 ²	Имя объекта	Char(10)	Имя объекта, который требуется расшифровать.
		695	Библиотека объекта	Char(10)	Библиотека объекта, который требуется расшифровать.
		705	Тип объекта	Char(8)	Тип объекта, который требуется расшифровать.
		713	Имя ASP ¹	Char(10)	Имя ASP.
		723	Номер ASP ¹	Char(5)	Номер ASP.
<p>¹ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p> <p>² Если имя объекта равно *N, а тип ошибки - S, то пользователь попытался расшифровать данные в переменной хоста.</p>					

Записи журнала RA (изменение прав доступа восстановленного объекта)

В этой таблице представлен формат записей журнала RA (изменение прав доступа восстановленного объекта).

Таблица 201. Записи журнала RA (изменение прав доступа восстановленного объекта). Файл описания полей QASYRAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение прав доступа восстановленного объекта
157	225	611	Имя объекта	Char(10)	Имя объекта.

Таблица 201. Записи журнала RA (изменение прав доступа восстановленного объекта) (продолжение). Файл описания полей QASYRAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Список прав доступа	Char(10)	Имя списка прав доступа.
195	263	649	Общие права доступа	Char(1)	Д Общие права доступа равны *EXCLUDE.
196	264	650	Частные права доступа	Char(1)	Д Частные права доступа удалены.
197	265	651	Удален список прав доступа	Char(1)	Д Из объекта удален список прав доступа.
198	266	652	(Зарезерв.)	Char(20)	
218	286	672	Имя DLO	Char(12)	Имя объекта библиотеки документов.
230	298	684	(Зарезерв.)	Char(8)	
238	306	692	Полное имя папки	Char(63)	Имя папки, содержащей объект библиотеки документов.
301			(Зарезерв.)	Char(20)	
	369	755	(Зарезерв.)	Char(18)	
	387	773	Длина имени объекта	Binary(4)	Длина имени объекта.
321	389	775	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
325	393	779	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
327	395	781	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
330	398	784	(Зарезерв.)	Char(3)	
333	401	787	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
349	417	803	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
365	433	819	Имя объекта ¹	Char(512)	Имя объекта.
	945	1331	ИД файла объекта	Char(16)	ИД файла объекта.
	961	1347	Имя ASP ⁵	Char(10)	Имя ASP.
	971	1357	Номер ASP ⁵	Char(5)	Номер ASP.
	976	1362	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.

Таблица 201. Записи журнала RA (изменение прав доступа восстановленного объекта) (продолжение). Файл описания полей QASYRAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	980	1366	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	982	1368	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	985	1371	Длина пути	Binary(4)	Длина имени пути.
	987	1373	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	988	1374	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1004	1390	Путь ⁴	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁵ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала RJ (восстановление описания задания)

В этой таблице представлен формат записей журнала RJ (восстановление описания задания).

Таблица 202. Записи журнала RJ (восстановление описания задания). Файл описания полей QASYRJJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.

Таблица 202. Записи журнала RJ (восстановление описания задания) (продолжение). Файл описания полей QASYRJJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Тип записи	Char(1)	Тип записи. A Восстановление описания задания, в параметре USER которого был задан пользовательский профайл.
157	225	611	Имя описания задания	Char(10)	Имя восстановленного описания задания.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, в которой восстановлено описание задания.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Имя польз.	Char(10)	Имя пользовательского профайла, указанное в описании задания.
		649	Имя ASP	Char(10)	Имя ASP библиотеки JOBD
		659	Номер ASP	Char(5)	Номер ASP библиотеки JOBD

Записи журнала RO (изменение владельца восстановленного объекта)

В этой таблице представлен формат записей журнала RO (изменение владельца восстановленного объекта).

Таблица 203. Записи журнала RO (изменение владельца восстановленного объекта). Файл описания полей QASYROJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Восстановление объектов, принадлежность которых изменяется при восстановлении
157	225	611	Имя объекта	Char(10)	Имя объекта.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, в которой расположен объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Прежний владелец	Char(10)	Имя прежнего владельца объекта.
195	263	649	Новый владелец	Char(10)	Имя нового владельца объекта.

Таблица 203. Записи журнала RO (изменение владельца восстановленного объекта) (продолжение). Файл описания полей QASYROJE/J4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
205	273	659	(Зарезерв.)	Char(20)	
225	293	679	Имя DLO	Char(12)	Имя объекта библиотеки документов.
237	305	691	(Зарезерв.)	Char(8)	
245	313	699	Полное имя папки	Char(63)	Папка, в которой был восстановлен объект.
308			(Зарезерв.)	Char(20)	
	376	762	(Зарезерв.)	Char(18)	
	394	780	Длина имени объекта ¹	Binary(4)	Длина имени объекта.
328	396	782	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
332	400	786	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
334	402	788	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
337	405	791	(Зарезерв.)	Char(3)	
340	408	794	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
356	424	810	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
372	440	826	Имя объекта ¹	Char(512)	Имя объекта.
	952	1338	ИД файла объекта	Char(16)	ИД файла объекта.
	968	1354	Имя ASP ⁵	Char(10)	Имя ASP.
	978	1364	Номер ASP ⁵	Char(5)	Номер ASP.
	983	1369	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	987	1373	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	989	1375	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	992	1378	Длина пути	Binary(4)	Длина имени пути.
	994	1380	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.

Таблица 203. Записи журнала RO (изменение владельца восстановленного объекта) (продолжение). Файл описания полей QASYROJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	995	1381	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1011	1397	Путь ⁴	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p> <p>⁵ Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.</p>					

Записи журнала RP (восстановление программ, принимающих права доступа)

В этой таблице представлен формат записей журнала RP (восстановление программ, принимающих права доступа).

Таблица 204. Записи журнала RP (восстановление программ, принимающих права доступа). Файл описания полей QASYRPJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Восстановление программ, принимающих права доступа владельца
157	225	611	Имя программы	Char(10)	Имя программы
167	235	621	Библиотека программы	Char(10)	Имя библиотеки, в которой расположена программа
177	245	631	Тип объекта	Char(8)	Тип объекта
185	253	639	Владелец	Char(10)	Имя владельца
	263	649	(Зарезерв.)	Char(18)	

Таблица 204. Записи журнала RP (восстановление программ, принимающих права доступа) (продолжение). Файл описания полей QASYRPJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	281	667	Длина имени объекта ¹	Binary (4)	Длина имени объекта.
	283	669	CCSID имени объекта ¹	Binary (5)	Идентификатор набора символов, связанный с именем объекта.
	287	673	ИД страны или региона для имени объекта ¹	Char (2)	ИД страны или региона, связанный с именем объекта.
	289	675	ИД языка для имени объекта ¹	Char (3)	ИД языка, связанный с именем объекта.
	292	678	(Зарезерв.)	Char (3)	
	295	681	ИД родительского файла ^{1,2}	Char (16)	ИД файла, связанный с родительским каталогом.
	311	697	ИД файла объекта ^{1,2}	Char (16)	ИД файла объекта.
	327	713	Имя объекта ¹	Char (512)	Имя объекта.
	839	1225	ИД файла объекта	Char(16)	ИД файла объекта.
	855	1241	Имя ASP ⁵	Char(10)	Имя ASP.
	865	1251	Номер ASP ⁵	Char(5)	Номер ASP.
	870	1256	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
I	874	1260	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
I	876	1262	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
I	879	1265	Длина пути	Binary(4)	Длина имени пути.
	881	1267	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	882	1268	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	898	1284	Путь ⁴	Char(5002)	Путь к объекту.

Таблица 204. Записи журнала RP (восстановление программ, принимающих права доступа) (продолжение). Файл описания полей QASYRPJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1					Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.
2					Если левый бит ИД равен единице, а остальные биты равны нулю, значит ИД не задан.
3					Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.
4					Это поле переменной длины. Длина пути указывается в первых двух байтах.
5					Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.

Записи журнала RQ (восстановление дескриптора запроса на изменение)

В этой таблице представлен формат записей журнала RQ (восстановление дескриптора запроса на изменение).

Таблица 205. Записи журнала RQ (восстановление дескриптора запроса на изменение). Файл описания полей QASYRQJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Восстановить объект *CRQD, принимающий права доступа.
157	225	611	Имя объекта	Char(10)	Имя дескриптора запроса на изменение.
167	235	621	Библиотека объекта	Char(10)	Имя библиотеки, содержащей дескриптор запроса на изменение.
177	245	631	Тип объекта	Char(8)	Тип объекта.
		639	Имя ASP	Char(10)	Имя ASP библиотеки CRQD
		649	Номер ASP	Char(5)	Номер ASP библиотеки CRQD

Записи журнала RU (восстановить права доступа пользовательского профайла)

В этой таблице представлен формат записей журнала RU (восстановить права доступа пользовательского профайла).

Таблица 206. Записи журнала RU (восстановить права доступа пользовательского профайла). Файл описания полей QASYRUJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Восстановление прав доступа пользовательских профайлов
157	225	611	Имя польз.	Char(10)	Имя пользовательского профайла, права доступа которого были восстановлены.
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки.
177	245	631	Тип объекта	Char(8)	Тип объекта.
	253	639	Права доступа восстановлены	Char(1)	Указывает, все ли права доступа пользователя были восстановлены. A Восстановлены все права доступа S Некоторые права доступа не восстановлены

Записи журнала RZ (изменение основной группы восстановленного объекта)

В этой таблице представлен формат записей журнала RZ (изменение основной группы восстановленного объекта).

Таблица 207. Записи журнала RZ (изменение основной группы восстановленного объекта). Файл описания полей QASYRZJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменена основная группа.

Таблица 207. Записи журнала RZ (изменение основной группы восстановленного объекта) (продолжение). Файл описания полей QASYRZJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
157	225	611	Имя объекта	Char(10)	Имя объекта.
167	235	621	Библиотека объекта	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Старая основная группа	Char(10)	Предыдущая основная группа объекта.
195	263	649	Новая основная группа	Char(10)	Новая основная группа объекта.
205	273	659	(Зарезерв.)	Char(20)	
225	293	679	Имя DLO	Char(12)	Имя объекта библиотеки документов.
237	305	691	(Зарезерв.)	Char(8)	
245	313	699	Полное имя папки	Char(63)	Папка, в которой был восстановлен объект.
308			(Зарезерв.)	Char(20)	
	376	762	(Зарезерв.)	Char(18)	
	394	780	Длина имени объекта ¹	Binary(4)	Длина имени объекта.
328	396	782	CCSID имени объекта ¹	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
332	400	786	ИД страны или региона для имени объекта ¹	Char(2)	ИД страны или региона, связанный с именем объекта.
334	402	788	ИД языка для имени объекта ¹	Char(3)	ИД языка, связанный с именем объекта.
337	405	791	(Зарезерв.)	Char(3)	
340	408	794	ИД родительского файла ^{1,2}	Char(16)	ИД файла, связанный с родительским каталогом.
356	424	810	ИД файла объекта ^{1,2}	Char(16)	ИД файла объекта.
372	440	826	Имя объекта ¹	Char(512)	Имя объекта.
	952	1338	ИД файла объекта	Char(16)	ИД файла объекта.
	968	1354	Имя ASP	Char(10)	Имя ASP.
	978	1364	Номер ASP	Char(5)	Номер ASP.
	983	1369	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	987	1373	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	989	1375	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.

Таблица 207. Записи журнала RZ (изменение основной группы восстановленного объекта) (продолжение). Файл описания полей QASYRZJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	992	1378	Длина пути	Binary(4)	Длина имени пути.
	994	1380	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	995	1381	Отн. ИД каталога ³	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ³
	1011	1397	Путь ⁴	Char(5002)	Путь к объекту.
<p>¹ Эти поля задаются только для объектов из файловой системы "root" (/), QOpenSys и пользовательских файловых систем.</p> <p>² Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>³ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁴ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p>					

Записи журнала SD (изменить системный каталог рассылки)

В этой таблице представлен формат записей журнала SD (изменить системный каталог рассылки).

Таблица 208. Записи журнала SD (изменить системный каталог рассылки). Файл описания полей QASYSDJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)" на стр. 594, "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)" на стр. 596 и "Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)" на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. S Изменение системного каталога

Таблица 208. Записи журнала SD (изменить системный каталог рассылки) (продолжение). Файл описания полей QASYSDJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
157	225	611	Тип изменения	Char(3)	ADD Добавить запись каталога CHG Изменить запись каталога COL Запись получателя DSP Показать запись каталога OUT Запрос к файлу вывода PRT Печать записи каталога RMV Удалить запись каталога RNM Переименовать запись каталога RTV Получить сведения SUP Запись поставщика
160	228	614	Тип записи	Char(4)	DIRE Каталог DPTD Сведения об отделе SHDW Теневая копия каталога SRCH Поиск в каталоге
164	232	618	Исходная система	Char(8)	Система, в которой внесено изменение
172	240	626	Пользовательский профайл	Char(10)	Пользовательский профайл, который внес изменение
182	250	636	Инициатор	Char(8)	Система, запросившая изменение
190	258	644	Запрошенная функция	Char(6)	INIT Инициализация OFFLIN Автономная инициализация REINIT Повторная инициализация SHADOW Обычное теневое копирование STPSHD Прервать теневое копирование
196	264	650	ИД пользователя	Char(8)	Изменяемый ИД пользователя
204	272	658	Адрес	Char(8)	Изменяемый адрес
212	280	666	Сетевой ИД пользователя	Char(47)	Изменяемый сетевой ИД пользователя

Записи журнала SE (изменение записи о выполнении подсистемы)

В этой таблице представлен формат записей журнала SE (изменение записи о выполнении подсистемы).

Таблица 209. Записи журнала SE (изменение записи о выполнении подсистемы). Файл описания полей QASYSEJE/J4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение записи о выполнении подсистемы
157	225	611	Имя подсистемы	Char(10)	Имя объекта
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, содержащей объект.
177	245	631	Тип объекта	Char(8)	Тип объекта.
185	253	639	Имя программы	Char(10)	Имя программы, изменившей запись о выполнении
195	263	649	Имя библиотеки	Char(10)	Имя библиотеки программы
205	273	659	Порядковый номер	Char(4)	Порядковый номер
209	277	663	Команда	Char(3)	Тип применявшейся команды ADD ADDRTGE CHG CHGRTGE RMV RMVRTGE
		666	Имя ASP библиотеки SBSD	Char(10)	Имя ASP библиотеки SBSD
		676	Номер ASP библиотеки SBSD	Char(5)	Номер ASP библиотеки SBSD
		681	Имя ASP библиотеки программ	Char(10)	Имя ASP библиотеки программ
		691	Номер ASP библиотеки программ	Char(5)	Номер ASP библиотеки программ

Записи журнала SF (действие над буферным файлом)

В этой таблице представлен формат записей журнала SF (действие над буферным файлом).

Таблица 210. Записи журнала SF (действие над буферным файлом). Файл описания полей QASYSFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип доступа	Char(1)	<p>Тип записи</p> <p>A Буферный файл прочитан кем-то, кроме его владельца.</p> <p>C Создание буферного файла.</p> <p>D Удаление буферного файла.</p> <p>H Блокирование буферного файла.</p> <p>I Создание внутреннего файла.</p> <p>Ч Разблокирование буферного файла.</p> <p>S Сохранение буферного файла.</p> <p>T Восстановление буферного файла.</p> <p>U Изменение атрибутов защиты буферного файла.</p> <p>V Изменение атрибутов буферного файла, не связанных с защитой.</p>
157	225	611	Имя файла базы данных	Char(10)	Имя файла базы данных, содержащего буферный файл
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки файла базы данных
177	245	631	Тип объекта	Char(8)	Тип объекта файла базы данных
185	253	639	Зарезерв. область	Char(10)	
195	263	649	Имя элемента	Char(10)	Имя элемента файла.
205	273	659	Имя буферного файла	Char(10)	Имя буферного файла ¹ .
215	283	669	Короткий номер буферного файла	Char(4)	Номер буферного файла ¹ . Если номер занимает более 4 байт, то это поле будет пустым, но будет задано значение в поле Номер буферного файла (J5, смещение 693).
219	287	673	Имя очереди вывода	Char(10)	Имя очереди вывода, содержащей буферный файл.
229	297	683	Библиотека очереди вывода	Char(10)	Имя библиотеки очереди вывода.
239			Зарезерв. область	Char(20)	

Таблица 210. Записи журнала SF (действие над буферным файлом) (продолжение). Файл описания полей QASYSFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	307	693	Номер буферного файла	Char(6)	Номер буферного файла.
	313	699	Зарезерв. область	Char(14)	
259	327	713	Старых копий	Char(3)	Число старых копий буферного файла
262	330	716	Новых копий	Char(3)	Число новых копий буферного файла
265	333	719	Старый принтер	Char(10)	Старый принтер буферного файла
275	343	729	Новый принтер	Char(10)	Новый принтер буферного файла
285	353	739	Новая очередь вывода	Char(10)	Новая очередь вывода буферного файла
295	363	749	Библиотека новой очереди вывода	Char(10)	Библиотека, содержащая новую очередь вывода
305	373	759	Старый тип формы	Char(10)	Старый тип формы буферного файла
315	383	769	Новый тип формы	Char(10)	Новый тип формы буферного файла
325	393	779	Старая начальная страница для повтора	Char(8)	Старая начальная страница для повтора печати буферного файла
333	401	787	Новая начальная страница для повтора	Char(8)	Новая начальная страница для повтора печати буферного файла
341	409	795	Старая начальная страница диапазона	Char(8)	Старая начальная страница диапазона буферного файла
349	417	803	Новая начальная страница диапазона	Char(8)	Новая начальная страница диапазона буферного файла
357	425	811	Старая конечная страница диапазона	Char(8)	Старая конечная страница диапазона буферного файла
365	433	819	Новая конечная страница диапазона	Char(8)	Новая конечная страница диапазона буферного файла
	441	827	Имя задания буферного файла	Char(10)	Имя задания буферного файла.

Таблица 210. Записи журнала SF (действие над буферным файлом) (продолжение). Файл описания полей QASYSFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	451	837	Пользователь задания буферного файла	Char(10)	Пользователь задания буферного файла.
	461	847	Номер задания буферного файла	Char(6)	Номер задания буферного файла.
	467	853	Старый лоток	Char(8)	Старый исходный лоток.
	475	861	Новый лоток	Char(8)	Новый исходный лоток.
	483	869	Имя старого определения страницы	Char(10)	Имя старого определения страницы.
	493	879	Библиотека старого определения страницы	Char(10)	Имя библиотеки старого определения страницы.
	503	889	Имя нового определения страницы	Char(10)	Имя нового определения страницы.
	513	899	Библиотека нового определения страницы	Char(10)	Имя библиотеки нового определения страницы.
	523	909	Имя старого определения формы	Char(10)	Имя старого определения формы.
	533	919	Библиотека старого определения формы	Char(10)	Имя библиотеки старого определения формы.
	543	929	Имя нового определения формы	Char(10)	Имя нового определения формы
	553	939	Библиотека нового определения формы	Char(10)	Имя библиотеки нового определения формы.
	563	949	Старая польз. опция 1	Char(10)	Старая польз. опция 1.
	573	959	Старая польз. опция 2	Char(10)	Старая польз. опция 2.
	583	969	Старая польз. опция 3	Char(10)	Старая польз. опция 3.
	593	979	Старая польз. опция 4	Char(10)	Старая польз. опция 4.
	603	989	Новая польз. опция 1	Char(10)	Новая польз. опция 1.

Таблица 210. Записи журнала SF (действие над буферным файлом) (продолжение). Файл описания полей QASYSFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	613	999	Новая польз. опция 2	Char(10)	Новая польз. опция 2.
	623	1009	Новая польз. опция 3	Char(10)	Новая польз. опция 3.
	633	1019	Новая польз. опция 4	Char(10)	Новая польз. опция 4.
	643	1029	Старый польз. объект	Char(10)	Имя старого пользовательского объекта.
	653	1039	Библиотека старого польз. объекта	Char(10)	Имя библиотеки старого пользовательского объекта.
	663	1049	Тип старого польз. объекта	Char(10)	Тип старого пользовательского объекта.
	673	1059	Новый польз. объект	Char(10)	Новый пользовательский объект.
	683	1069	Библиотека нового польз. объекта	Char(10)	Имя библиотеки нового пользовательского объекта.
	693	1079	Тип нового польз. объекта	Char(10)	Тип нового пользовательского объекта.
	703	1089	Имя системы задания буферного файла	Char(8)	Имя системы, в которой хранится буферный файл.
	711	1097	Дата создания буферного файла	Char(7)	Дата создания буферного файла (ВГГММДД).
	718	1104	Время создания буферного файла	Char(6)	Время создания буферного файла (ЧЧММСС).
		1110	Имя старых польз. данных	Char(255)	Имя старых польз. данных
		1365	Имя новых польз. данных	Char(255)	Имя новых польз. данных
		1620	Имя ASP файла	Char(10)	Имя ASP библиотеки файла базы данных.
		1630	Номер ASP файла	Char(5)	Номер ASP библиотеки файла базы данных.
		1635	Имя ASP очереди вывода	Char(10)	Имя ASP библиотеки очереди вывода.
		1645	Номер ASP очереди вывода	Char(5)	Номер ASP библиотеки очереди вывода.
		1650	Имя ASP новой очереди вывода	Char(10)	Имя ASP библиотеки новой очереди вывода.
		1660	Номер ASP новой очереди вывода	Char(5)	Номер ASP библиотеки новой очереди вывода.

Таблица 210. Записи журнала SF (действие над буферным файлом) (продолжение). Файл описания полей QASYSFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		1665	Прежнее состояние буферного файла	Char(3)	Прежнее состояние буферного файла.
		1668	Новое состояние буферного файла	Char(3)	Новое состояние буферного файла.
		1671	Дата первоначального создания	Char(7)	Дата первоначального создания.
		1678	Время первоначального создания	Char(6)	Время первоначального создания.
		1684	Дата истечения срока действия прежнего буферного файла	Char(7)	Дата истечения срока действия прежнего буферного файла
		1687	Дата истечения срока действия нового буферного файла	Char(7)	Дата истечения срока действия нового буферного файла
		1694	Дата создания буферного файла, UTC	Char(7)	Дата создания буферного файла в UTC. (Совпадает с датой создания буферного файла (смещение 1097), но указывается в UTC)
		1701	Время создания буферного файла, UTC	Char(6)	Время создания буферного файла в UTC. (Совпадает с временем создания буферного файла (смещение 1104), но указывается в UTC)
¹ Это поле пусто, если тип записи равен I (печать в файл).					

Записи журнала SG (асинхронные сигналы)

В этой таблице представлен формат записей журнала SG (асинхронные сигналы).

Таблица 211. Записи журнала SG (асинхронные сигналы). Файл описания полей QASYSGJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.

Таблица 211. Записи журнала SG (асинхронные сигналы) (продолжение). Файл описания полей QASYSGJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	224	610	Тип записи	Char(1)	Тип записи. A Обработан асинхронный сигнал i5/OS P Обработан асинхронный сигнал PASE
	225	611	Номер сигнала	Char(4)	Номер обработанного сигнала.
	229	615	Действие по обработке	Char(1)	Действие, выполненное при получении сигнала. C Выполнение процесса продолжено E Создана исключительная ситуация H Вызвана функция обработки сигналов S Процесс остановлен T Процесс завершен U Выполнение запроса завершено
	230	616	Источник сигнала	Char(1)	Источник сигнала. M Система P Процесс Примечание: Если источник сигнала - система, то атрибуты исходного задания не указываются.
	231	617	Имя исходного задания	Char(10)	Первый компонент полного имени исходного задания.
	241	627	Имя пользователя исходного задания	Char(10)	Второй компонент полного имени исходного задания.
	251	637	Номер исходного задания	Char(6)	Третий компонент полного имени исходного задания.
	257	643	Текущий пользователь исходного задания	Char(10)	Текущий пользовательский профайл, связанный с исходным заданием.
	267	653	Время создания	Char(8)	Время создания сигнала в формате *DTS. Примечание: Для преобразования значения *DTS в другие форматы можно воспользоваться API QWCCVTDT.

Записи журнала SK (соединения SSL)

В этой таблице представлен формат записей журнала SK (соединения SSL).

Таблица 212. Записи журнала SK (соединения SSL). Файл описания полей QASYSKJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.
	224	610	Тип записи	Char(1)	A Принято C Соединение D Присвоен адрес DHCP F Фильтрованная почта P Порт недоступен Ч Почта отклонена U Адрес DHCP не присвоен
	225	611	Локальный IP-адрес ³	Char(15)	IP-адрес локальной системы.
	240	626	Локальный порт	Char(5)	Локальный порт.
	245	631	Удаленный IP-адрес ³	Char(15)	IP-адрес удаленной системы.
	260	646	Удаленный порт	Char(5)	Удаленный порт.
	265	651	Дескриптор сокета	Bin(5)	Дескриптор сокета.
	269	655	Описание фильтра	Char(10)	Указанный фильтр почты.
	279	665	Длина данных фильтра	Bin(4)	Длина данных фильтра.
	281	667	Данные фильтра ¹	Char(514)	Данные фильтра.
	795	1181	Семейство адресов	Char(10)	Семейство адресов. *IPv4 Протокол IP версии 4 *IPv6 Протокол IP версии 6
	805	1191	Локальный IP-адрес	Char(46)	IP-адрес локальной системы.
	851	1237	Удаленный IP-адрес ²	Char(46)	Удаленный IP-адрес
	897	1283	Адрес MAC	Char(32)	Адрес MAC клиента, отправившего запрос.
	929	1315	Имя хоста	Char(255)	Имя хоста клиента, отправившего запрос.
¹	Это поле переменной длины. Длина поля указывается в первых двух байтах.				
²	Если тип записи равен D, то это поле содержит IP-адрес, который был присвоен клиенту сервером DHCP.				
³	В этих полях разрешено указывать только адреса IPv4.				

Записи журнала SM (изменение параметров управления системами)

В этой таблице представлен формат записей журнала SM (изменение параметров управления системами).

Таблица 213. Записи журнала SM (изменение параметров управления системами). Файл описания полей QASYSMJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Запрошенная функция B Изменен список резервного копирования C Опции автоматической очистки D DRDA F Файловая система HFS Нет Операция над сетевым файлом O Изменены опции резервного копирования P Расписание включения-выключения питания S Системный список ответов T Изменено время восстановления путей доступа
157	225	611	Тип доступа	Char(1)	A Добавление C Изменение D Удаление Ч Удаление S Просмотр T Получение
158	226	612	Порядковый номер	Char(4)	Порядковый номер действия
162	230	616	ИД сообщения	Char(7)	ИД сообщения, связанного с действием
169	237	623	Имя реляционной базы данных	Char(18)	Имя реляционной базы данных
187	255	641	Имя файловой системы	Char(10)	Имя файловой системы

Таблица 213. Записи журнала SM (изменение параметров управления системами) (продолжение). Файл описания полей QASYSMJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
197	265	651	Измененная опция резервного копирования	Char(10)	Опция резервного копирования, которая была изменена
207	275	661	Измененный список резервного копирования	Char(10)	Список резервного копирования, который был изменен
217	285	671	Имя сетевого файла	Char(10)	Имя применявшегося сетевого файла
227	295	681	Элемент сетевого файла	Char(10)	Имя элемента сетевого файла
237	305	691	Номер сетевого файла	Zoned(6,0)	Номер сетевого файла
243	311	697	Владелец сетевого файла	Char(10)	Имя пользовательского профайла, которому принадлежит сетевой файл
253	321	707	Пользователь - источник сетевого файла	Char(8)	Имя пользовательского профайла, от которого был получен сетевой файл
261	329	715	Адрес - источник сетевого файла	Char(8)	Адрес, с которого был получен сетевой файл

Записи журнала SO (действия над пользовательской информацией о защите сервера)

В этой таблице представлен формат записей журнала SO (действия над пользовательской информацией о защите сервера).

Таблица 214. Записи журнала SO (действия над пользовательской информацией о защите сервера). Файл описания полей QASYSOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 214. Записи журнала SO (действия над пользовательской информацией о защите сервера) (продолжение). Файл описания полей QASYSOJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Тип записи	Char(1)	Тип записи A Добавить запись C Изменить запись Ч Удалить запись T Получить запись
157	225	611	Пользовательский профайл	Char(10)	Имя пользовательского профайла.
	235	621	Тип записи польз. информации	Char(1)	Нет Тип записи не задан. U Запись содержит информацию о пользовательском приложении. Д Запись содержит идентификационную информацию сервера.
	236	622	Пароль сохранен	Char(1)	Нет Пароль не сохранен S Без изменения Д Пароль сохранен
	237	623	Имя сервера	Char(200)	Имя сервера.
	437	823	(Зарезерв.)	Char(3)	
	440	826	Длина ИД пользователя	Binary (4)	Длина ИД пользователя.
	442	828	(Зарезерв.)	Char(20)	
	462	848	ИД пользователя	Char(1002) ¹	Идентификатор пользователя.

¹ Это поле переменной длины. Длина поля указывается в первых двух байтах.

Записи журнала ST (обращение к сервисным средствам)

В этой таблице представлен формат записей журнала ST (обращение к сервисным средствам).

Таблица 215. Записи журнала ST (обращение к сервисным средствам). Файл описания полей QASYSTJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 215. Записи журнала ST (обращение к сервисным средствам) (продолжение). Файл описания полей QASYSTJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Тип записи	Char(1)	Тип записи A Запись о службе
157	225	611	Сервисное средство	Char(2)	Тип записи. AN ANZJVM AR Диагностическая трассировка ARM (см. команду ARMSRV QShell) CD QTACTLDV, QTADMPDV CE QWTCTLTR CS STRCPYSCN CT DMPCLUTRC DC DLTCMNTRC DD DMPDLO DF QWTDMPFR, QWTDMPFL DI QSCDIRD DJ DMPJVM, QPYRTJVM DM DMPMEMINF DO DMPOBJ
					DS DMPYSOBY, QTADMPTS, QTADMPDV, QWTDMPFL DU DMPUSRPRF DW STRDW, ENDDW, ADDDWDFN, RMVDWDFN EC ENDCMNTRC ER ENDRMTSPT GS QSMGSSTD HD QYHCHCOP (DASD) HL QYHCHCOP (LPAR)
					JW STRJW, ENDJW, ADDJWDFN, RMVJWDFN LC EPT создан LD EPT удален LE EPT задания изменен LF Системный EPT зафиксирован LG Записи EPT были изменены LH Выполнено сравнение EPT

Таблица 215. Записи журнала ST (обращение к сервисным средствам) (продолжение). Файл описания полей QASYSTJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
					LI Показаны записи EPT MC QWTMAINT (изменение) MD QWTMAINT (дамп) MP Завершить системное задание MQ Перезапустить системное задание OP Консоль управления PC PRTCMNTRC
					PE PRTERLOG, QTADMPDV PI PRTINTDTA, QTADMPDV PS QP0FPTOS SC STRCMNTRC SE QWTSETTR
					SF QWCCDSIC, QWVRCSTK (Показать запись внутреннего стека) SJ STRSRVJOB SN QPZSYNC SR STRRMTSPT SS QFPHPSF ST STRSST SV QRSRV TA TRCTCPAPP
					TC TRCCNN (задано значение *FORMAT) TE ENDTRC, ENDPEX, TRCJOB(указано *OFF или *END) TI TRCINT или TRCCNN с SET(*ON), SET(*OFF) или SET(*END) TO QTOBSRV TQ QWCTMQTM TS STRTRC, STRPEX, TRCJOB(указано *ON)
					UD QTAUPDDV WE ENDWCH, QSCWCH WS STRWCH, QSCSWCH WT WRKTRC WW WRKWCH
159	227	613	Имя объекта	Char(10)	Имя запрошенного объекта

Таблица 215. Записи журнала ST (обращение к сервисным средствам) (продолжение). Файл описания полей QASYSTJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
169	237	623	Имя библиотеки	Char(10)	Имя библиотеки объекта
179	247	633	Тип объекта	Char(8)	Тип объекта
187	255	641	Имя задания	Char(10)	Первый компонент полного имени задания
197	265	651	Имя пользователя задания	Char(10)	Второй компонент полного имени задания
207	275	661	Номер задания	Zoned(6,0)	Третий компонент полного имени задания
213	281	667	Имя объекта	Char(30)	Имя объекта для DMPSYSOBJ
243	311	697	Имя библиотеки	Char(30)	Имя библиотеки объекта для DMPSYSOBJ
273	341	727	Тип объекта	Char(8)	Тип объекта
281	349	735	Имя DLO	Char(12)	Имя объекта библиотеки документов
293	361	747	(Зарезерв.)	Char(8)	
301	369	755	Путь к папке ⁸	Char(63)	Папка, содержащая объект библиотеки документов
	432	818	Поле JUID	Char(10)	JUID целевого задания
	442	828	Действие для предв. трассировки ¹	Char(10)	Действие, выполнение которого запрошено для предварительной трассировки задания *ON Предварительная трассировка включена *OFF Предварительная трассировка выключена *RESET Предварительная трассировка выключена. Информация трассировки удалена.
	452	838	Опция трассировки приложения ²	Char(1)	Опция трассировки, заданная в TRCTCPAPP. A ⁶ Активировать D ⁶ Деактивировать Y ⁷ Начат сбор информации трассировки N ⁷ Сбор информации трассировки прекращен. Информация трассировки записана в буферный файл E ⁷ Сбор информации трассировки прекращен. Информация трассировки очищена (вывод не создан)
	453	839	Приложение для трассировки ²	Char(10)	Имя приложения, трассировка которого выполнялась.
	463	849	Профайл сервисных средств ³	Char(10)	Имя профайла сервисных средств, применявшегося для STRSST.

Таблица 215. Записи журнала ST (обращение к сервисным средствам) (продолжение). Файл описания полей QASYSTJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		859	ИД исходного узла	Char(8)	ИД исходного узла
		867	Исходный пользователь	Char(10)	Исходный пользователь
		877	Имя ASP библиотеки объекта	Char(10)	Имя ASP библиотеки объекта
		887	Номер ASP библиотеки объекта	Char(5)	Номер ASP библиотеки объекта
		892	Имя ASP библиотеки объекта DMPSYSOBJ	Char(10)	Имя ASP библиотеки объекта DMPSYSOBJ
		902	Номер ASP библиотеки объекта DMPSYSOBJ	Char(5)	Номер ASP библиотеки объекта DMPSYSOBJ
		907	Тип консоли ⁴	Char(10)	Тип консоли. Возможны следующие значения: <ul style="list-style-type: none"> • *DIRECT • *LAN • *HMC
		917	Действие консоли ⁴	Char(10)	Действие консоли. Возможны следующие значения: <ul style="list-style-type: none"> • *RECOVERY • *TAKEOVER
		927	Семейство адресов ⁴	Char(10)	Семейство адресов. <ul style="list-style-type: none"> • *IPv4 • *IPv6
		937	Предыдущий IP-адрес ⁴	Char(46)	IP-адрес предыдущей консоли для *LAN.
		938	ИД предыдущего устройства ⁴	Char(10)	ИД устройства сервисных средств предыдущей консоли для *LAN.
		993	Текущий IP-адрес ⁴	Char(46)	IP-адрес текущей консоли для *LAN.
		1039	ИД текущего устройства ⁴	Char(10)	ИД устройства сервисных средств текущей консоли для *LAN.
		1049	Сеанс слежения ⁵	Char(10)	ИД сеанса слежения.
		1059	Запись ⁹	Char(10)	Имя записи в таблице входных точек изменено.

Таблица 215. Записи журнала ST (обращение к сервисным средствам) (продолжение). Файл описания полей QASYSTJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		1069	Связанный объект ¹⁰	Char(10)	Имя связанного объекта. <ul style="list-style-type: none"> Для значения LC сервисного средства это поле содержит имя базовой таблицы точек входа. Для значения LG сервисного средства это поле содержит имя замещающей программы. Для значения LH сервисного средства это поле содержит имя базовой таблицы точек сравнения.
		1079	Библиотека связанных объектов ¹⁰	Char(10)	Имя библиотеки связанных объектов. <ul style="list-style-type: none"> Для значения LC сервисного средства это поле содержит имя библиотеки базовой таблицы точек входа. Для значения LG сервисного средства это поле содержит имя библиотеки замещающей программы. Для значения LH сервисного средства это поле содержит имя библиотеки базовой таблицы точек сравнения.
1	Это поле применяется только в том случае, когда значение сервисных средств равно CE (тип задается в поле со смещением 611).				
2	Это поле применяется только в том случае, когда значение сервисных средств равно AR или TA (тип задается в поле со смещением 611).				
3	Это поле применяется только в том случае, когда значение сервисных средств равно ST или OP (тип задается в поле со смещением 611).				
4	Это поле применяется только в том случае, когда значение сервисных средств равно OP (тип задается в поле со смещением 611).				
5	Это поле применяется только в том случае, когда значение сервисных средств равно WS или WE (тип задается в поле со смещением 611).				
6	Это поле применяется только в том случае, когда значение сервисных средств равно AR (тип задается в поле со смещением 611).				
7	Это поле применяется только в том случае, когда значение сервисных средств равно TA (тип задается в поле со смещением 611).				
8	Путь к папке будет содержать 30-символьную команду расширенного анализа, когда значение сервисных средств равно AR (тип задается в поле со смещением 611).				
9	Это поле применяется только в том случае, когда значение сервисных средств равно LG (тип задается в поле со смещением 611).				
10	Это поле применяется только в том случае, когда значение сервисных средств равно LC, LG или LH (тип задается в поле со смещением 611).				

Записи журнала SV (действие над системным значением)

В этой таблице представлен формат записей журнала SV (действие над системным значением).

Таблица 216. Записи журнала SV (действие над системным значением). Файл описания полей QASYSVJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи. A Изменение системных значений B Изменение служебных атрибутов C Изменение системного времени D Разница с временем UTC E Изменение опции F Изменение атрибута системного журнала
157	225	611	Системное значение или служебный атрибут	Char(10)	JRNRCVCNT Изменено значение числа восстановлений журнала MAXCCHWAIT Изменено значение максимального времени ожидания кэша журнала QINPIDCO Изменение текущей опции конфигурации диска установки с помощью QINPIDCO API.
167	235	621	Новое значение	Char(250)	Новое значение, присвоенное системному значению или служебному атрибуту
417	485	871	Старое значение	Char(250)	Старое значение системного значения или служебного атрибута
667	735	1121	Продолжение нового значения	Char(250)	Продолжение значения, которое было присвоено системному значению или служебному атрибуту.
917	985	1371	Продолжение старого значения	Char(250)	Продолжение значения, которое раньше было присвоено системному значению или служебному атрибуту.
		1621	Расширение продолжения нового значения	Char(1000)	Второе продолжение значения, которое было присвоено системному значению или служебному атрибуту
		2621	Расширение продолжения прежнего значения	Char(1000)	Второе продолжение значения, которое раньше было присвоено системному значению или служебному атрибуту.

Записи журнала VA (изменение списка управления доступом)

В этой таблице представлен формат записей журнала VA (изменение списка управления доступом).

Таблица 217. Записи журнала VA (изменение списка управления доступом). Файл описания полей QASYVAJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Состояние	Char(1)	Состояние запроса. S Успешное F Не выполнен
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, отправившего запрос на изменение списка управления доступом.
187	255	641	Имя инициатора запроса	Char(10)	Имя пользователя, отправившего запрос.
197	265	651	Выполненное действие	Char(1)	Действие, выполненное в профайле управления доступом: A Добавление C Модификация D Удаление
198	266	652	Имя ресурса	Char(260)	Имя измененного ресурса.

Записи журнала VC (запуск и завершение соединения)

В этой таблице представлен формат записей журнала VC (запуск и завершение соединения).

Таблица 218. Записи журнала VC (запуск и завершение соединения). Файл описания полей QASYVCJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Действие над соединением.	Char(1)	Выполненное действие над соединением. S Запуск E Завершение Ч Отклонено
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, отправившего запрос на изменение состояния соединения.
187	255	641	Пользователь соединения	Char(10)	Имя пользователя, связанное с запросом на изменение состояния соединения.
197	265	651	ИД соединения	Char(5)	ИД запущенного или завершенного соединения.
202	270	656	Причина отклонения	Char(1)	Причина отклонения соединения: A Автоматическое отключение (тайм-аут), удаление общего ресурса или отсутствие прав администратора E Ошибка, отключение сеанса или неверный пароль Нет Обычное отключение или превышение ограничения, заданного для имени пользователя P Нет прав доступа к общему ресурсу
203	271	657	Имя сети	Char(12)	Имя сети, связанное с соединением.

Записи журнала VF (закрытие файлов сервера)

В этой таблице представлен формат записей журнала VF (закрытие файлов сервера).

Таблица 219. Записи журнала VF (закрытие файлов сервера). Файл описания полей QASYVFJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Причина закрытия	Char(1)	Причина закрытия файла. A Административное отключение Нет Обычное отключение клиента S Отключение сеанса
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, отправившего запрос на закрытие.
187	255	641	Пользователь соединения	Char(10)	Имя пользователя, отправившего запрос на закрытие.
197	265	651	ИД файла	Char(5)	ИД закрытого файла.
202	270	656	Продолж.	Char(6)	Время в секундах, в течение которого файл был открыт.
208	276	662	Имя ресурса	Char(260)	Имя ресурса, которому принадлежит файл.

Записи журнала VL (превышено ограничение для учетной записи)

В этой таблице представлен формат записей журнала VL (превышено ограничение для учетной записи).

Таблица 220. Записи журнала VL (превышено ограничение для учетной записи). Файл описания полей QASYVLJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 220. Записи журнала VL (превышено ограничение для учетной записи) (продолжение). Файл описания полей QASYVLJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Причина	Char(1)	Причина превышения ограничения. A Истек срок действия учетной записи D Учетная запись заблокирована L Превышено ограничение на время работы в системе U Неизвестна или недоступна W Недопустимая рабочая станция
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, на котором превышено ограничение для учетной записи.
187	255	641	Пользователь (User)	Char(10)	Имя пользователя, связанное с превышением ограничения для учетной записи.
197	265	651	Имя ресурса	Char(260)	Имя применявшегося ресурса.

Записи журнала VN (вход в сеть и выход из нее)

В этой таблице представлен формат записей журнала VN (вход в сеть и выход из нее).

Таблица 221. Записи журнала VN (вход в сеть и выход из нее). Файл описания полей QASYVNJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип события	Char(1)	Тип зарегистрированного события: F Запрошен выход из сети O Запрошен вход в сеть Ч Запрос на вход в сеть отклонен
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.

Таблица 221. Записи журнала VN (вход в сеть и выход из нее) (продолжение). Файл описания полей QASYVNJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
179	247	633	Имя компьютера	Char(8)	Имя компьютера, с которым связано событие.
187	255	641	Пользователь (User)	Char(10)	Пользователь, вошедший в сеть или вышедший из нее.
197	265	651	Права доступа пользователя	Char(1)	Права доступа пользователя, вошедшего в сеть: A Администратор G Гость U Пользователь (User)
198	266	652	Причина отклонения	Char(1)	Причина отклонения запроса на вход в сеть: A Доступ запрещен F Превышено ограничение на вход в сеть P Неверный пароль
199	267	653	Доп. причина	Char(1)	Сведения о том, почему был запрещен доступ: A Истек срок действия учетной записи D Учетная запись заблокирована L Неверное время входа в систему Ч Неверный ИД инициатора U Неизвестна или недоступна

Записи журнала VO (контрольный список)

В этой таблице представлен формат записей журнала VO (контрольный список).

Таблица 222. Записи журнала VO (контрольный список). Формат описания полей QASYVOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596.

Таблица 222. Записи журнала VO (контрольный список) (продолжение). Формат описания полей QASYVOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	224	610	Тип записи	Char(1)	Тип записи. A Добавить запись контрольного списка C Изменить запись контрольного списка F Найти запись контрольного списка Ч Удалить запись контрольного списка U Неудачная проверка записи контрольного списка V Удачная проверка записи контрольного списка
	225	611	Тип ошибки	Char(1)	Тип неудачной проверки. E Неверные зашифрованные данные I Не найдена запись с указанным ИД V Не найден контрольный список
	226	612	Контрольный список	Char(10)	Имя контрольного списка.
	236	622	Имя библиотеки	Char(10)	Имя библиотеки, в которой расположен контрольный список.
	246	632	Зашифрованные данные	Char(1)	Данные, которые должны быть зашифрованы. Д Данные для шифрования были указаны в запросе. Нет Данные для шифрования не были указаны в запросе.
	247	633	Данные записи	Char(1)	Данные записи. Д Данные записи были указаны в запросе. Нет Данные записи не были указаны в запросе.
	248	634	Длина ИД записи	Binary(4)	Длина идентификатора записи.
	250	636	Длина данных	Binary(4)	Длина данных записи.
	252	638	Атрибут зашифрованных данных	Char (1)	Зашифрованные данные. ' ' Атрибут зашифрованных данных не был задан. 0 Данные, которые должны быть зашифрованы, могут применяться только для проверки записи. Преобразование выполняется по умолчанию. 1 Данные, которые должны быть зашифрованы, могут применяться для проверки записи. Кроме того, их можно возвращать в результатах поиска.
	253	639	Атрибут сертификата X.509	Char (1)	Сертификат X.509.

Таблица 222. Записи журнала VO (контрольный список) (продолжение). Формат описания полей QASYVOJ4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	254	640	(Зарезерв.)	Char (28)	
	282	668	ИД записи	Byte(100)	Идентификатор записи.
	382	768	Данные записи	Byte(1000)	Данные записи.
		1768	Имя ASP библиотеки контрольного списка	Char(10)	Имя ASP библиотеки контрольного списка
		1778	Номер ASP библиотеки контрольного списка	Char(5)	Номер ASP библиотеки контрольного списка

Записи журнала VP (ошибка в сетевом пароле)

В этой таблице представлен формат записей журнала VP (ошибка в сетевом пароле).

Таблица 223. Записи журнала VP (ошибка в сетевом пароле). Файл описания полей QASYVPJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип ошибки	Char(1)	Тип возникшей ошибки. P Ошибка в пароле
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, отправившего запрос.
187	255	641	Пользователь (User)	Char(10)	Имя пользователя, попытавшегося войти в сеть.

Записи журнала VR (обращение к сетевому ресурсу)

В этой таблице представлен формат записей журнала VR (обращение к сетевому ресурсу).

Таблица 224. Записи журнала VR (обращение к сетевому ресурсу). Файл описания формата QASYVRJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Состояние	Char(1)	Состояние запроса на доступ к ресурсу. F Доступ к ресурсу отклонен S Доступ к ресурсу предоставлен
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, обратившегося к ресурсу.
187	255	641	Пользователь (User)	Char(10)	Имя пользователя, обратившегося к ресурсу.
197	265	651	Тип операции	Char(1)	Тип выполненной операции: A Изменены атрибуты ресурса C Создан экземпляр ресурса D Ресурс удален P Изменены права доступа к ресурсу Ч Из ресурса прочитаны данные W В ресурс записаны данные X Ресурс запущен
198	266	652	Код возврата	Char(4)	Код возврата, полученный в том случае, если доступ к ресурсу был предоставлен.
202	270	656	Сообщение сервера	Char(4)	Код сообщения, отправленного после предоставления доступа.
206	274	660	ИД файла	Char(5)	ИД запрошенного файла.
211	279	665	Имя ресурса	Char(260)	Имя применявшегося ресурса.

Записи журнала VS (сеанс сервера)

В этой таблице представлен формат записей журнала VS (сеанс сервера).

Таблица 225. Записи журнала VS (сеанс сервера). Файл описания полей QASYVSJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Действие над сеансом	Char(1)	Выполненное действие над сеансом. E Сеанс завершен S Сеанс запущен
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, запросившего сеанс.
187	255	641	Пользователь (User)	Char(10)	Имя пользователя, запросившего сеанс.
197	265	651	Права доступа пользователя	Char(1)	Уровень прав доступа пользователя, необходимый для запуска сеанса: A Администратор G Гость U Пользователь (User)
198	266	652	Код причины	Char(1)	Код причины завершения сеанса. A Сеанс отключен администратором D Автоматическое отключение (тайм-аут), удаление общего ресурса или отсутствие прав администратора E Ошибка, отключение сеанса или неверный пароль Нет Обычное отключение или превышение ограничения, заданного для имени пользователя Ч Ограничение учетной записи

Записи журнала VU (изменение сетевого профайла)

В этой таблице представлен формат записей журнала VU (изменение сетевого профайла).

Таблица 226. Записи журнала VU (изменение сетевого профайла). Файл описания полей QASYVUJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594; “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип	Char(1)	Тип измененной записи. G Запись группы U Запись пользователя M Глобальная информация о пользовательском профайле
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, запросившего изменение пользовательского профайла
187	255	641	Пользователь (User)	Char(10)	Имя пользователя, запросившего изменение пользовательского профайла.
197	265	651	Действие	Char(1)	Запрошенное действие: A Добавление C Изменение D Удаление P Неверный пароль
198	266	652	Имя ресурса	Char(260)	Имя ресурса.

Записи журнала VV (изменение состояния службы)

В этой таблице представлен формат записей журнала VV (изменение состояния службы).

Таблица 227. Записи журнала VV (изменение состояния службы). Файл описания полей QASYVVJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Тип записи: C Изменилось состояние службы E Сервер остановлен P Сервер приостановлен Ч Сервер перезапущен S Сервер запущен
157	225	611	Имя сервера	Char(10)	Имя описания сетевого сервера, зарегистрировавшего событие.
167	235	621	Дата на сервере	Char(6)	Дата регистрации события на сетевом сервере.
173	241	627	Время на сервере	Zoned(6,0)	Время регистрации события на сетевом сервере.
179	247	633	Имя компьютера	Char(8)	Имя компьютера, отправившего запрос на изменение.
187	255	641	Пользователь (User)	Char(10)	Имя пользователя, отправившего запрос на изменение.
197	265	651	Состояние	Char(1)	Состояние в запросе к службе: A Служба активна B Запуск службы - ожидание C Возобновление работы службы E Завершение ожидания службы H Приостанов службы I Служба приостановлена S Служба остановлена
198	266	652	Код службы	Char(8)	Код запрошенной службы.
206	274	660	Текст	Char(80)	Текст, заданный в запросе к службе.
286	354	740	Возвращенное значение	Char(4)	Значение, возвращенное операцией изменения.
290	358	744	Служба	Char(20)	Измененная служба.

Записи журнала X0 (сетевая идентификация)

В этой таблице представлен формат записей журнала X0 (сетевая идентификация).

Таблица 228. Записи журнала X0 (сетевая идентификация). Файл описания полей QASYX0JE/J4/J5

Смещ.			Поле	Отформатирован	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.

Таблица 228. Записи журнала X0 (сетевая идентификация) (продолжение). Файл описания полей QASYX0JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
156	224	610	Тип записи	Char(1)	<p>Тип записи:</p> <p>1 Служебный паспорт действителен</p> <p>2 Субъекты служб не совпадают.</p> <p>3 Субъекты клиентов не совпадают.</p> <p>4 Несовпадение IP-адреса паспорта.</p> <p>5 Не удалось расшифровать паспорт.</p> <p>6 Не удалось расшифровать систему идентификации</p> <p>7 Область не входит в локальные области клиента</p> <p>8 Попытка использования паспорта для имитации.</p> <p>9 Паспорт еще не действителен.</p> <p>A Ошибка при расшифровке контрольной суммы KRB_AP_PRIV или KRB_AP_SAFE</p> <p>B Несовпадение IP-адреса удаленной системы</p> <p>C Несовпадение IP-адреса локальной системы</p> <p>D Ошибка метки времени KRB_AP_PRIV или KRB_AP_SAFE</p> <p>E Ошибка повторного использования KRB_AP_PRIV или KRB_AP_SAFE</p> <p>F Неверный порядок KRB_AP_PRIV или KRB_AP_SAFE</p> <p>K Подтверждение GSS — истек срок действия разрешения</p> <p>L Подтверждение GSS — ошибка в контрольной сумме</p> <p>M Подтверждение GSS — связывание канала</p> <p>Нет Развертывание GSS или проверка с помощью GSS, информация с истекшим сроком действия.</p> <p>O Развертывание GSS или проверка с помощью GSS, расшифровка.</p> <p>P Развертывание GSS или проверка с помощью GSS, ошибка в контрольной сумме.</p> <p>Q Развертывание GSS или проверка с помощью GSS, ошибка в последовательности.</p>
	225	611	Код состояния	Char(8)	Состояние запроса

Таблица 228. Записи журнала X0 (сетевая идентификация) (продолжение). Файл описания полей QASYX0JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	233	619	Значение состояния GSS	Char(8)	Значение состояния GSS
	241	627	Удаленный IP-адрес	Char(21)	Удаленный IP-адрес
	262	648	Локальный IP-адрес	Char(21)	Локальный IP-адрес
	283	669	Зашифрованные адреса	Char(256)	Зашифрованные IP-адреса
	539	925	Индикатор зашифрованных адресов	Char(1)	Индикатор зашифрованных IP-адресов Д указаны все адреса Нет указаны не все адреса Х не предоставлен
	540	926	Флаги паспорта	Char(8)	Флаги паспорта
	548	934	Время идентификации паспорта	Char(8)	Время идентификации паспорта
	556	942	Время начала действия паспорта	Char(8)	Время начала действия паспорта
	564	950	Время окончания действия паспорта	Char(8)	Время окончания действия паспорта
	572	958	Время обновления паспорта	Char(8)	Время, до наступления которого нужно обновить паспорт
	580	966	Системное время сообщения	Char(8)	Системное время X0E
	588	974	Системное время истечения срока действия GSS	Char(8)	Системное время истечения срока действия контекста или разрешения GSS
	596	982	CCSID субъекта сервера	Binary(5)	CCSID субъекта сервера, полученного из паспорта
	600	986	Длина имени субъекта сервера	Binary(4)	Длина имени субъекта сервера, полученного из паспорта
	602	988	Индикатор субъекта сервера	Char(1)	Индикатор субъекта сервера, полученного из паспорта Д субъект сервера задан полностью Нет субъект сервера задан неполностью Х не предоставлен
	603	989	Субъект сервера	Char(512)	Субъект сервера, полученный из паспорта

Таблица 228. Записи журнала X0 (сетевая идентификация) (продолжение). Файл описания полей QASYX0JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	1115	1501	CCSID параметра субъекта сервера	Binary(5)	CCSID параметра субъекта сервера, полученного из паспорта
	1119	1505	Длина параметра субъекта сервера	Binary(4)	Длина параметра субъекта сервера, полученного из паспорта
	1121	1507	Индикатор параметра субъекта сервера	Char(1)	Индикатор параметра субъекта сервера, полученного из паспорта Д субъект сервера задан полностью Нет субъект сервера задан неполностью X не предоставлен
	1122	1508	Параметр субъекта сервера	Char(512)	Параметр субъекта сервера, которому должен соответствовать паспорт
	1634	2020	CCSID субъекта клиента	Binary(5)	CCSID субъекта клиента, полученного от службы идентификации
	1638	2024	Длина имени субъекта клиента	Binary(4)	Длина имени субъекта клиента, полученного от службы идентификации
	1640	2026	Индикатор субъекта клиента	Char(1)	Индикатор субъекта клиента, полученного от службы идентификации Д субъект клиента задан полностью Нет субъект клиента задан неполностью X не предоставлен
	1641	2027	Субъект клиента	Char(512)	Субъект клиента, полученный от службы идентификации
	2153	2539	CCSID субъекта клиента	Binary(5)	CCSID субъекта клиента, полученного из паспорта
	2157	2543	Длина имени субъекта клиента	Binary(4)	Длина имени субъекта клиента, полученного из паспорта
	2159	2545	Индикатор субъекта клиента	Char(1)	Индикатор субъекта клиента, полученного из паспорта Д субъект клиента задан полностью Нет субъект клиента задан неполностью X не предоставлен
	2160	2546	Субъект клиента	Char(512)	Субъект клиента, полученный из паспорта
	2672	3058	CCSID субъекта сервера GSS	Binary(5)	CCSID субъекта сервера, полученного из разрешения GSS

Таблица 228. Записи журнала X0 (сетевая идентификация) (продолжение). Файл описания полей QASYX0JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	2676	3062	Длина имени субъекта сервера GSS	Binary(4)	Длина имени субъекта сервера, полученного из разрешения GSS
	2678	3064	Индикатор субъекта сервера GSS	Char(1)	Индикатор субъекта сервера, полученного из разрешения GSS Д субъект сервера задан полностью Нет субъект сервера задан неполностью Х не предоставлен
	2679	3065	Субъект сервера GSS	Char(512)	Субъект сервера из разрешения GSS
	3191	3577	CCSID локального субъекта GSS	Binary(5)	CCSID имени локального субъекта GSS
	3195	3581	Длина имени локального субъекта GSS	Binary(4)	Длина имени локального субъекта GSS
	3197	3583	Индикатор локального субъекта GSS	Char(1)	Индикатор имени локального субъекта GSS Д имя локального субъекта задано полностью Нет имя локального субъекта задано неполностью Х не предоставлен
	3198	3584	Локальный субъект GSS	Char(512)	Локальный субъект GSS
	3710	4096	CCSID удаленного субъекта GSS	Binary(5)	CCSID имени удаленного субъекта GSS
	3714	4100	Длина имени удаленного субъекта GSS	Binary(4)	Длина имени удаленного субъекта GSS
	3716	4102	Индикатор удаленного субъекта GSS	Char(1)	Индикатор имени удаленного субъекта GSS Д имя удаленного субъекта задано полностью Нет имя удаленного субъекта задано неполностью Х не предоставлен
	3717	4103	Удаленный субъект GSS	Char(512)	Удаленный субъект GSS

Записи журнала X1 (идентификационный маркер)

В этой таблице представлен формат записей журнала X1 (идентификационный маркер).

Таблица 229. Записи журнала X1 (идентификационный маркер). Файл описания полей QASYX1JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
		610	Тип записи	Char(1)	<p>Тип записи:</p> <p>D Идентификационный маркер успешно передан</p> <p>F Идентификационный маркер не передан</p> <p>G Из идентификационного маркера получено имя пользователя</p> <p>U Из идентификационного маркера не получено имя пользователя</p>
		611	Код причины	Binary (5)	<p>Код причины, по которой запрос не был выполнен:</p> <p>9 Неправильная длина маркера</p> <p>10 Неправильный идентификатор EIM</p> <p>11 Неправильный ИД экземпляра приложения</p> <p>12 Недопустимая подпись маркера</p> <p>13 Недопустимый идентификационный маркер</p> <p>14 Не найден целевой пользователь</p> <p>16 Не найден описатель ключа</p> <p>17 Версия маркера не поддерживается</p> <p>18 Не найден общий ключ</p> <p>Примечание: В случае сбоя в текстовых полях будет сохранена только та информация, которая была проверена к моменту сбоя.</p>
		615	Зарезерв.	Char(7)	Зарезерв.
		622	CCSID данных	Binary(5)	CCSID данных в текстовых полях
		626	Длина имени получателя	Binary(5)	Длина данных в поле Получатель.
		630	Получатель	Char(508)	Получатель идентификационного маркера, запрос которого был обработан или не был выполнен. Данные в этом поле задаются в следующем формате: <EIMID>ИД-получателя-в-EIM </EIMID> <APPID>ИД-приложения-получателя </APPID> <TIMESTAMP>системное-время-получателя </TIMESTAMP>. Системное время указывается только для запросов о передаче маркера.
		1138	Длина имени отправителя	Binary(5)	Длина данных в поле Отправитель.

Таблица 229. Записи журнала X1 (идентификационный маркер) (продолжение). Файл описания полей QASYX1JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		1142		Char(508)	Последний отправитель идентификационного маркера, запрос которого был обработан или не был выполнен. Данные в этом поле задаются в следующем формате: <EIMID>ИД-отправителя-в-EIM</EIMID> <APPID>ИД-приложения-отправителя</APPID> <TIMESTAMP>системное-время-отправителя</TIMESTAMP>
		1650	Длина имени инициатора	Binary(5)	Длина данных в поле Инициатор.
		1654	Инициатор	Char(508)	Инициатор запроса на получение идентификационного маркера. Если отправитель и получатель совпадают, то длина этого поля будет равна 0. Данные в этом поле задаются в следующем формате: <EIMID>ИД-инициатора-в-EIM</EIMID> <APPID>ИД-приложения-инициатора</APPID> <TIMESTAMP>системное-время-инициатора</TIMESTAMP>
		2162	Длина данных о цепочке	Binary(5)	Длина данных в поле Цепочка.
		2166	Цепочка	Char(2036)	Цепочка отправителей между инициатором и последним получателем. Цепочка начинается с последнего и заканчивается первым получателем. Если других получателей нет, то длина данных в этом поле будет равна 0. Цепочка усекается, если ее длина превосходит длину поля. Данные в этом поле задаются в следующем формате: <SNDRz><EIMID>sndrz_eimID</EIMID> <APPID>sndrz_appID</APPID> <TIMESTAMP>системное-время-sndrz </TIMESTAMP> </SNDRz> <SNDRy>...</SNDRy>...
		4202	Записей в цепочке	Binary(5)	Число записей в поле Цепочка.
		4206	Доступно записей в цепочке	Binary(5)	Число записей, доступных в цепочке получателей. Это значение может превосходить число записей в поле Цепочка, если цепочка была усечена по размеру поля.
		4210	Длина имени исходного реестра	Binary(5)	Длина данных в поле Исходный реестр.
		4214	Исходный реестр	Char(508)	Исходный реестр, указанный в маркере идентификации.
		4722	Длина имени пользователя из исходного реестра	Binary(5)	Длина данных в поле Пользователь исходного реестра.
		4726	Пользователь исходного реестра	Char(508)	Пользователь из исходного реестра, указанный в идентификационном маркере.
		5234	Длина имени целевого реестра	Binary(5)	Длина данных в поле Целевой реестр.
		5238	Целевой реестр	Char(508)	Указанный целевой реестр.

Таблица 229. Записи журнала X1 (идентификационный маркер) (продолжение). Файл описания полей QASYX1JE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		5746	Длина имени пользователя из целевого реестра	Binary(5)	Длина данных в поле Пользователь целевого реестра.
		5750	Пользователь целевого реестра	Char(508)	Пользователь из целевого реестра, которому соответствует идентификационный маркер.

Записи журнала XD (расширение сервера каталогов)

В этой таблице представлен формат записей журнала XD (расширение сервера каталогов).

Таблица 230. Записи журнала XD (расширение сервера каталогов). Файл описания поля QASYXDJ5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
		610	Тип записи	Char(1)	Тип записи: G Имена групп. Имена групп перечислены в полях с 1 по 5.
		611	Перекрестная ссылка	Char(36)	Строка перекрестной ссылки, применяемая для связи этой записи с записями DI с помощью этих групп. На эту запись XD может ссылаться несколько записей DI, если несколько запросов LDAP используют один и тот же набор групп.
		647	Зарезерв.	Char(100)	
		747	CCSID поля 1	Bin(5)	Значение CCSID для поля 1.
		751	Длина поля 1	Bin(4)	Длина данных в поле 1.
		753	Поле 1	Char(2002)	Данные поля 1 Для типа записи G в этом поле содержится имя группы из подтверждения членства в группе.
		2755	CCSID поля 2	Bin(5)	Значение CCSID для поля 2.
		2759	Длина поля 2	Bin(4)	Длина данных в поле 2.
		2761	Поле 2	Char(2002)	Данные поля 2 Для типа записи G в этом поле содержится имя группы из подтверждения членства в группе.
		4763	CCSID поля 3	Bin(5)	Значение CCSID для поля 3.
		4767	Длина поля 3	Bin(4)	Длина данных в поле 3.

Таблица 230. Записи журнала XD (расширение сервера каталогов) (продолжение). Файл описания поля QASYXDJ5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
		4769	Поле 3	Char(2002)	Данные поля 3 Для типа записи G в этом поле содержится имя группы из подтверждения членства в группе.
		6771	CCSID поля 4	Bin(5)	Значение CCSID для поля 4.
		6775	Длина поля 4	Bin(4)	Длина данных в поле 4.
		6777	Поле 4	Char(2002)	Данные поля 4 Для типа записи G в этом поле содержится имя группы из подтверждения членства в группе.
		8779	CCSID поля 5	Bin(5)	Значение CCSID для поля 5.
		8783	Длина поля 5	Bin(4)	Длина данных в поле 5.
		8785	Поле 5	Char(2002)	Данные поля 5 Для типа записи G в этом поле содержится имя группы из подтверждения членства в группе.

Записи журнала YC (изменение объекта DLO)

В этой таблице представлен формат записей журнала YC (изменение объекта DLO).

Таблица 231. Записи журнала YC (изменение объекта DLO). Файл описания полей QASYJCJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Доступ к объекту C Изменение объекта DLO
157	225	611	Имя объекта	Char(10)	Имя объекта
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки
177	245	631	Тип объекта	Char(8)	Тип объекта
185	253	639	Польз. Office	Char(10)	Профайл пользователя Office
195	263	649	Имя документа или папки	Char(12)	Имя документа или папки
207	275	661	(Зарезерв.)	Char(8)	
215	283	669	Полное имя папки	Char(63)	Папка, содержащая объект библиотеки документов

Таблица 231. Записи журнала YC (изменение объекта DLO) (продолжение). Файл описания полей QASYCJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
278	346	732	Пользователь, от имени которого выполняется работа	Char(10)	Пользователь, от имени которого работает другой пользователь
288	356	742	Тип доступа	Packed(5,0)	Тип доступа ¹
¹ Список типов доступа приведен в разделе “Коды типов доступа” на стр. 745.					

Записи журнала YR (чтение объекта DLO)

В этой таблице представлен формат записей журнала YR (чтение объекта DLO).

Таблица 232. Записи журнала YR (чтение объекта DLO). Файл описания полей QASYRJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Доступ к объекту Ч Чтение объекта DLO
157	225	611	Имя объекта	Char(10)	Имя объекта
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки
177	245	631	Тип объекта	Char(8)	Тип объекта
185	253	639	Польз. Office	Char(10)	Профайл пользователя Office
195	263	649	Имя документа или папки	Char(12)	Имя объекта библиотеки документов
207	275	661	(Зарезерв.)	Char(8)	
215	283	669	Полное имя папки	Char(63)	Папка, содержащая объект библиотеки документов
278	346	732	Пользователь, от имени которого выполняется работа	Char(10)	Пользователь, от имени которого работает другой пользователь
288	356	742	Тип доступа	Packed(5,0)	Тип доступа ¹
¹ Список типов доступа приведен в разделе “Коды типов доступа” на стр. 745.					

Записи журнала ZC (изменение объекта)

В этой таблице представлен формат записей журнала ZC (изменение объекта).

Таблица 233. Записи журнала ZC (изменение объекта). Файл описания полей QASYZCJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Доступ к объекту C Изменение объекта U Расширение открытого доступа к объекту
157	225	611	Имя объекта	Char(10)	Имя объекта
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, в которой расположен объект
177	245	631	Тип объекта	Char(8)	Тип объекта
185	253	639	Тип доступа	Packed(5,0)	Тип доступа ¹

Таблица 233. Записи журнала ZC (изменение объекта) (продолжение). Файл описания полей QASYZCJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
188	256	642	Сведения о доступе	Char(50)	<p>Сведения о доступе</p> <p>Если тип объекта равен *IMGCLG, то данные в этом поле задаются в следующем формате:</p> <p>Char 3 Индекс записи каталога образов.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Char 32 ИД тома записи каталога образов.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Char 1 Тип доступа к записи. Возможные значения указаны ниже.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Ч Файл, содержащий запись каталога образов, доступен только для чтения.</p> <p>W Файл, содержащий запись каталога образов, доступен для чтения и записи.</p> <p>Char 1 Состояние защиты от записи для записи каталога образов.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Д Файл, содержащий запись каталога образов, защищен от записи.</p> <p>Нет Файл, содержащий запись каталога образов, не защищен от записи.</p> <p>Char 10 Имя виртуального накопителя.</p> <p>Blank Операция выполнялась над каталогом образов, либо каталог образов не готов к работе.</p> <p>Char 3 Не применяется.</p> <p>Если тип объекта - это объект интегрированной файловой системы, то в этом поле содержится дополнительная информация о запросе на изменение. Возможные значения описаны в файле QPOLJRNЛ.H QSYSINC.</p>
238			(Зарезерв.)	Char(20)	
	306	692	(Зарезерв.)	Char(18)	

Таблица 233. Записи журнала ZC (изменение объекта) (продолжение). Файл описания полей QASYZCJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
	324	710	Длина имени объекта ²	Binary(4)	Длина имени объекта.
258	326	712	CCSID имени объекта ²	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
262	330	716	ИД страны или региона для имени объекта ²	Char(2)	ИД страны или региона, связанный с именем объекта.
264	332	718	ИД языка для имени объекта ²	Char(3)	ИД языка, связанный с именем объекта.
267	335	721	(Зарезерв.)	Char(3)	
270	338	724	ИД род. каталога ^{2,3}	Char(16)	ИД файла, связанный с родительским каталогом.
286	354	740	ИД файла объекта ^{2,3}	Char(16)	ИД файла объекта.
302	370	756	Имя объекта ²	Char(512)	Имя объекта.
	882	1268	ИД файла объекта	Char(16)	ИД файла объекта.
	898	1284	Имя ASP ⁶	Char(10)	Имя ASP.
	908	1294	Номер ASP ⁶	Char(5)	Номер ASP.
	913	1299	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	917	1303	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	919	1305	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	922	1308	Длина пути	Binary(4)	Длина имени пути.
	924	1310	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	925	1311	Отн. ИД каталога ⁴	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ⁴
	941	1327	Путь ⁵	Char(5002)	Путь к объекту.

Таблица 233. Записи журнала ZC (изменение объекта) (продолжение). Файл описания полей QASYZCJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1					Список типов доступа приведен в разделе “Коды типов доступа” на стр. 745.
2					Эти поля задаются только для объектов из файловой системы “root” (/), QOpenSys и пользовательских файловых систем.
3					Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.
4					Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.
5					Это поле переменной длины. Длина пути указывается в первых двух байтах.
6					Если объект расположен в библиотеке, то информация об ASP относится к библиотеке. В противном случае информация об ASP относится к самому объекту.

Записи журнала ZR (чтение объекта)

В этой таблице представлен формат записей журнала ZR (чтение объекта).

Таблица 234. Записи журнала ZR (чтение объекта). Файл описания полей QASYZRJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
1	1	1			Поля заголовка, общие для записей всех типов. Описание полей приведено в разделах “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE5 (*TYPE5)” на стр. 594, “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE4 (*TYPE4)” на стр. 596 и “Стандартные поля заголовков для записей журнала контроля Формат записи QJORDJE2 (*TYPE2)” на стр. 597.
156	224	610	Тип записи	Char(1)	Доступ к объекту Ч Чтение объекта
157	225	611	Имя объекта	Char(10)	Имя объекта
167	235	621	Имя библиотеки	Char(10)	Имя библиотеки, в которой расположен объект
177	245	631	Тип объекта	Char(8)	Тип объекта
185	253	639	Тип доступа	Packed(5,0)	Тип доступа ¹

Таблица 234. Записи журнала ZR (чтение объекта) (продолжение). Файл описания полей QASYZRJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
188	256	642	Сведения о доступе	Char(50)	<p>Сведения о доступе.</p> <p>Если тип объекта равен *IMGCLG, то данные в этом поле задаются в следующем формате:</p> <p>Char 3 Индекс записи каталога образов.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Char 32</p> <p>ИД тома записи каталога образов.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Char 1 Тип доступа к записи. Возможные значения указаны ниже.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Ч Файл, содержащий запись каталога образов, доступен только для чтения.</p> <p>W Файл, содержащий запись каталога образов, доступен для чтения и записи.</p> <p>Char 1 Состояние защиты от записи для записи каталога образов.</p> <p>Blank Операция выполнялась над каталогом образов.</p> <p>Д Файл, содержащий запись каталога образов, защищен от записи.</p> <p>Нет Файл, содержащий запись каталога образов, не защищен от записи.</p> <p>Char 10</p> <p>Имя виртуального накопителя.</p> <p>Blank Операция выполнялась над каталогом образов, либо каталог образов не готов к работе.</p> <p>Char 3 Не применяется.</p>
238			(Зарезерв.)	Char(20)	
	306	692	(Зарезерв.)	Char(18)	
	324	710	Длина имени объекта ²	Binary(4)	Длина имени объекта.
258	326	712	CCSID имени объекта ²	Binary(5)	Идентификатор набора символов, связанный с именем объекта.
262	330	716	ИД страны или региона для имени объекта ²	Char(2)	ИД страны или региона, связанный с именем объекта.

Таблица 234. Записи журнала ZR (чтение объекта) (продолжение). Файл описания полей QASYZRJE/J4/J5

Смещ.			Поле	Отформатировано	Описание
JE	J4	J5			
264	332	718	ИД языка для имени объекта ²	Char(3)	ИД языка, связанный с именем объекта.
267	335	721	(Зарезерв.)	Char(3)	
270	338	724	ИД родительского файла ^{2,3}	Char(16)	ИД файла, связанный с родительским каталогом.
286	354	740	ИД файла объекта ^{2,3}	Char(16)	ИД файла объекта.
302	370	756	Имя объекта ²	Char(512)	Имя объекта.
	882	1268	ИД файла объекта	Char(16)	ИД файла объекта.
	898	1284	Имя ASP	Char(10)	Имя ASP.
	908	1294	Номер ASP	Char(5)	Номер ASP.
	913	1299	CCSID пути к объекту	Binary(5)	Идентификатор набора символов, связанный с путем.
	917	1303	ИД страны или региона для пути к объекту	Char(2)	ИД страны или региона, связанный с именем пути.
	919	1305	ИД языка для пути к объекту	Char(3)	ИД языка, связанный с именем пути.
	922	1308	Длина пути	Binary(4)	Длина имени пути.
	924	1310	Индикатор пути	Char(1)	Индикатор пути: Д Поле Путь содержит полное имя объекта. Нет Поле Путь содержит не полное, а относительное имя объекта. Полный путь может быть образован с помощью этого поля и поля Относительный ИД каталога.
	925	1311	Отн. ИД каталога ⁴	Char(16)	Если в поле Индикатор пути указано N, то данное поле содержит ИД каталога для объекта, указанного в поле Путь. В противном случае оно содержит шестнадцатеричные нули. ⁴
	941	1327	Путь ⁵	Char(5002)	Путь к объекту.
<p>¹ Список типов доступа приведен в разделе “Коды типов доступа”.</p> <p>² Эти поля задаются только для объектов из файловой системы “root” (/), QOpenSys и пользовательских файловых систем.</p> <p>³ Если первый разряд ИД равен 1, а остальные - 0, значит ИД не задан.</p> <p>⁴ Если в поле Индикатор пути указано N, но поле Относительный ИД каталога заполнено шестнадцатеричными нулями, то при определении пути произошла ошибка.</p> <p>⁵ Это поле переменной длины. Длина пути указывается в первых двух байтах.</p>					

Коды типов доступа

В этой таблице перечислены коды доступа, применяемые в записях журнала контроля из файлов QASYUCJE/J4/J5, QASYURJE/J4/J5, QASYZCJE/J4/J5 и QASYZRJE/J4/J5.

Таблица 235. Коды типов доступа

Код	Тип доступа	Код	Тип доступа	Код	Тип доступа
1	Добавление	26	Загрузка	51	Отправка
2	Активация программы	27	Просмотр списка	52	Запуск
3	Анализ	28	Перемещение	53	Передача
4	Применение	29	Объединение	54	Трассировка
5	Вызов или TFRCTL	30	Открытие	55	Проверка
6	Настройка	31	Печать	56	Изменение состояния
7	Изменение	32	Запрос	57	Work
8	Контроль	33	Восстановление	58	Чтение/изменение атрибута DLO
9	Закрытие	34	Получение	59	Чтение/изменение параметров защиты DLO
10	Очистить	35	Чтение	60	Чтение/изменение содержимого DLO
11	Сравнение	36	Реорганизация	61	Чтение изменение всех компонентов DLO
12	Отмена	37	Разблокирование	62	Добавление ограничения
13	Копирование	38	Удаление	63	Изменение ограничения
14	Создание	39	Переименование	64	Удаление ограничения
15	Преобразование	40	Замена	65	Запуск процедуры
16	Отладка	41	Возобновление	66	Получение доступа к **ООPOOL
17	Удаление	42	Восстановить	67	Создание подписи объекта
18	Создать дампы	43	Получение	68	Удаление всех подписей
19	Просмотр	44	Запуск	69	Очистка объекта с подписью
20	Редактирование	45	Аннулирование прав	70	Монтирование
21	Завершение	46	Сохранить	71	Выгрузка
22	Файл	47	Сохранение с освобождением памяти	72	Завершение отката
23	Предоставление прав	48	Сохранение и удаление		
24	Блокировка	49	Передача на выполнение		
25	Инициализация	50	Настройка		

Таблица 235. Коды типов доступа (продолжение)

Код	Тип доступа	Код	Тип доступа	Код	Тип доступа

Приложение G. Команды и меню защиты

Для настройки защиты системы применяются следующие инструменты: меню SECTOOLS (Инструменты защиты), меню SECBATCH (Запустить или запланировать обработку отчетов в пакетном режиме), команды Настроить защиту системы (CFGSYSSEC) и Аннулировать общие права доступа (RVKPUBAUT).

При работе с инструментами защиты можно применять два меню:

- Меню SECTOOLS (Инструменты защиты) для интерактивного выполнения команд.
- Меню SECBATCH (Запустить или запланировать обработку отчетов в пакетном режиме) для выполнения команд вывода отчетов в пакетном режиме. Меню SECBATCH состоит из двух частей. В первой части доступна команда Передать задание на выполнение (SBMJOB) для немедленной обработки отчетов в пакетном режиме.

Во второй части меню доступна команда Добавить запись расписания заданий (ADDJOBSCDE). Она служит для планирования регулярной обработки отчетов о защите в указанные дни и часы.

Опции меню Инструменты защиты

Меню Инструменты защиты (SECTOOLS) упрощает управление защитой системы. Оно содержит различные опции и команды.

Ниже показана часть меню SECTOOLS, имеющая отношение к пользовательским профайлам.

Для перехода к этому меню введите команду GO SECTOOLS.

SECTOOLS	Инструменты защиты
Выберите один из следующих вариантов:	
Работа с профайлами	
1. Анализировать пароли по умолчанию	
2. Показать список активных профайлов	
3. Изменить список активных профайлов	
4. Анализировать операции профайлов	
5. Показать расписания активации	
6. Изменить запись расписания активации	
7. Показать расписание истечения срока	
8. Изменить запись расписания истечения срока	
9. Печать внутренних значений профайлов	

В Табл. 236 приведено описание этих опций меню и связанных с ними команд:

Таблица 236. Команды для пользовательских профайлов

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
1	ANZDFTPWD	С помощью команды Анализировать пароли по умолчанию вы можете определить пользовательские профайлы, у которых пароль совпадает с их именем, и выполнить над такими профайлами заданное действие.	QASECPWD ²

Таблица 236. Команды для пользовательских профайлов (продолжение)

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
2	DSPACTPRFL	С помощью команды Показать список активных профайлов вы можете просмотреть или напечатать список пользовательских профайлов, которые не будут обрабатываться командой ANZPRFACT.	QASECIDL ²
3	CHGACTPRFL	С помощью команды Изменить список активных профайлов вы можете добавлять и удалять пользовательские профайлы в список исключений для команды ANZPRFACT. Пользовательские профайлы, включенные в список активных профайлов, считаются постоянно активными (до того момента, пока вы не удалите их из списка). Команда ANZPRFACT не отключает профайл, включенный в список активных профайлов, независимо от того, сколько времени он бездействует.	QASECIDL ²
4	ANZPRFACT	Команда Анализировать операции профайлов служит для отключения пользовательских профайлов, которые не применялись в течение указанного числа дней. После того как вы зададите число дней для команды ANZPRFACT, система будет каждую ночь запускать задание ANZPRFACT. С помощью команды CHGACTPRFL можно настроить исключения для некоторых пользовательских профайлов.	QASECIDL ²
5	DSPACTSCD	С помощью команды Показать расписание активации можно просмотреть или напечатать расписание активации и отключения конкретных пользовательских профайлов. Это расписание задается командой CHGACTSCDE.	QASECACT ²
6	CHGACTSCDE	С помощью команды Изменить запись расписания активации можно настроить пользовательский профайл таким образом, чтобы он будет доступен только в определенное время дня и в определенные дни недели. Для каждого профайла, включенного в расписание, система создает записи расписания заданий с указанием времени его включения и отключения.	QASECACT ²
7	DSPEXPSCDE	С помощью команды Показать расписание истечения срока можно просмотреть или напечатать список пользовательских профайлов, для которых запланировано отключение или удаления из системы. Срок действия профайлов задается командой CHGEXPSCDE.	QASECEXP ²

Таблица 236. Команды для пользовательских профайлов (продолжение)

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
8	CHGEXPSCDE	<p>С помощью команды Изменить запись расписания истечения срока можно запланировать удаление пользовательского профайла. Вы можете временно отключить профайл или совсем удалить его из системы. Эта команда использует запись расписания заданий, запускаемую каждые сутки в 00:01. Задание считывает файл QASECEXP и определяет, истекает ли срок действия какого-либо профайла в этот день.</p> <p>Просмотреть список пользовательских профайлов, для которых запланировано истечение срока действия, можно с помощью команды DSPEXPSCD.</p>	QASECEXP ²
9	PRTPRFINT	С помощью команды Печатать содержимое профайла можно напечатать отчет с указанием числа записей объекта пользовательского профайла (*USRPRF).	
<p>Notes:</p> <p>1. Опции меню SECTOOLS.</p> <p>2. Файл находится в библиотеке QUSRSYS.</p>			

Для просмотра дополнительных опций меню нажмите клавишу Page down. В Табл. 237 описаны опции меню и связанные с ними команды, служащие для контроля действий:

Таблица 237. Команды для контроля за действиями

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
10	CHGSECAUD	<p>Команда Изменить параметры контроля действий служит для настройки контроля действий и для изменения соответствующих системных значений. Если в момент запуска команды CHGSECAUD журнал контроля действий (QAUDJRN) в системе не существует, то он автоматически создается.</p> <p>У команды CHGSECAUD есть несколько опций, упрощающих настройку системных значений QAUDLVL (Уровень контроля) и QAUDLVL2 (Расширение уровня контроля). Поддерживается значение *ALL, позволяющее включить все возможные параметры контроля. Значение *DFTSET позволяет включить наиболее часто используемые параметры (*AUTFAIL, *CREATE, *DELETE, *SECURITY и *SAVRST).</p> <p>Примечание: Если для настройки контроля действий вы применяете инструменты защиты, то рекомендуется запланировать управление получателями журнала контроля. В противном случае быстро возникнет проблема нехватки дискового пространства.</p>	

Таблица 237. Команды для контроля за действиями (продолжение)

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
11	DSPSECAUD	Команда Показать параметры контроля действий служит для просмотра информации о журнале контроля действий и о соответствующих системных значениях.	
12	CPYAUDJRNE	Команда Скопировать записи журнала контроля служит для копирования записей из журнала контроля за действиями в файл вывода.	QASYxxJ5 ²
¹ Опции меню SECTOOLS. ² xx - это тип записи журнала, длиной в два символа. Например, файл вывода для записей журнала типа AE будет выглядеть как QSYS/QASYAEJ5. Модели файлов вывода описаны в Приложение F, "Макет записей журнала контроля", на стр. 593 данной книги.			

Применение меню защиты в пакетном режиме

Меню защиты в пакетном режиме позволяет передать один или несколько отчетов инструментов защиты в очередь для последующего выполнения в пакетном режиме. Можно запланировать передачу пакетного задания на выполнение один раз, либо через определенные интервалы. В этом разделе приведены примеры работы с этим меню.

Ниже приведена первая часть меню SECWATCH:

```
SECWATCH Запустить или заплан. обработку отчетов защиты в пакетном режиме
Система:
```

Выберите один из следующих вариантов:

Передать отчеты на обработку в пакетном режиме

1. Принимающие объекты
2. Записи журнала контроля
3. Права доступа к списку прав доступа
4. Права доступа к команде
5. Частные права доступа к команде
6. Защита средств связи
7. Права доступа к каталогу
8. Частные права доступа к каталогу
9. Права доступа к документу
10. Частные права доступа к документу
11. Права доступа к файлам
12. Частные права доступа к файлу
13. Права доступа к папке

При выборе опции этого меню появляется показанное ниже меню Передать задание на выполнение (SBMJOB).

```

                                Передать задание на выполнение (SBMJOB)
Введите опции, нажмите Enter.

Команда . . . . . > PRTADPOBJ USRPRF(*ALL)
_____
_____
...
Имя задания . . . . . *JOBД          Имя, *JOBД
Описание задания . . . . . *USRPRF     Имя, *USRPRF
Библиотека . . . . . _____        Имя, *LIBL, *CURLIB
Очередь задания . . . . . *JOBД        Имя, *JOBД
Библиотека . . . . . _____        Имя, *LIBL, *CURLIB
Приоритет задания (в JOBQ) . . . . . *JOBД      1-9, *JOBД
Приоритет вывода (в OUTQ) . . . . . *JOBД      1-9, *JOBД
Устройство вывода . . . . . *CURRENT      Имя, *CURRENT, *USRPRF...

```

Если вы хотите изменить применяемые по умолчанию опции команды, то нажмите F4 (Приглашение) в строке *Вызываемая команда*.

Для просмотра расписания обработки отчетов в пакетном режиме нажмите клавишу Page down в меню SECWATCH. С помощью опций этой части меню можно, например, настроить регулярный запуск отчетов об изменениях в системе.

```

SECWATCH  Запустить или заплан. обработку отчетов защиты в пакетном режиме
                                                Система:
Выберите один из следующих вариантов:

    28. Пользовательские объекты
    29. Информация о пользовательских профайлах
    30. Внутренние объекты пользовательских профайлов
    31. Проверка целостности объектов
Расписание пакетных отчетов
    40. Принимающие объекты
    41. Записи журнала контроля
    42. Права доступа к списку прав доступа
    43. Права доступа к команде
    44. Частные права доступа к команде
    45. Защита средств связи
    46. Права доступа к каталогу

```

Для перехода к дополнительным опциям меню нажмите клавишу Page down. При выборе одной из опций этого раздела меню появится меню Добавить запись расписания заданий (ADDJOBSCDE):

```

                                Добавить запись расписания заданий (ADDJOBSCDE)
Введите опции, нажмите Enter.

Имя задания . . . . . _____        Имя, *JOBД
Команда . . . . . > PRTADPOBJ USRPRF(*ALL)
_____
_____
_____
...
Частота . . . . . _____        *ONCE, *WEEKLY, *MONTHLY
Запланированная дата или . . . . . *CURRENT      Дата, *CURRENT, *MONTHST
День . . . . . *NONE                *NONE, *ALL, *MON, *TUE.
+ доп. значения
Запланированное время . . . . . *CURRENT      Время, *CURRENT

```

Для выбора других значений поместите курсор на строку *Вызываемая команда* и нажмите F4 (Приглашение). Заданию следует присвоить значимое имя, по которому вы сможете впоследствии распознать эту запись среди других записей расписания заданий.

Опции меню SECWATCH

В этом разделе описаны опции меню и связанные с ними команды, служащие для обработки отчетов о защите.

При вызове команд работы с отчетами о защите система печатает только ту информацию, которая отвечает указанным вами критериям выбора и критериям выбора применяемого инструмента. Например, описания задания, в которых указано имя пользовательского профайла, требуют настройки защиты. В связи с этим отчет с описанием задания (PRTJOBDAUT) печатается в указанной библиотеке только в том случае, если данному описанию задания не присвоены права доступа *EXCLUDE и если в описании задания в параметре USER указан пользовательский профайл.

Аналогично, при печати информации о подсистеме (команда PRTSBSDAUT) система печатает эту информация только в том случае, если в описание подсистемы включена запись средств связи, задающая пользовательский профайл.

Если в какой-либо отчет было включено меньше информации, чем вы ожидали, то обратитесь к электронной справке и определите критерии выбора для этого отчета.

Таблица 238. Команды работы с отчетами о защите

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
1, 40	PRTADPOBJ	С помощью команды Печать принимающих объектов можно напечатать список объектов, принимающих права доступа указанного пользовательского профайла. Вы можете указать отдельный профайл, шаблон имен профайлов (например, все имена, начинающиеся с буквы Q) или все профайлы системы. Возможны два варианта вывода этого отчета. Полный отчет включает список всех принимающих объектов, отвечающих заданным условиям выбора. В отчете об изменениях перечислены различия между принимающими объектами, находящимися в системе в настоящий момент, и принимающими объектами, которые находились в системе в момент предыдущей обработки этого отчета.	QSECADPOLD ²
2, 41	DSPAUDJRNE ⁶	Команда Показать записи журнала контроля служит для просмотра или печати информации о записях журнала контроля действий. Вы можете выбрать группу записей по типу, по пользователям или по интервалу времени.	QASYxxJ5 ³

Таблица 238. Команды работы с отчетами о защите (продолжение)

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
3, 42	PRTPVTAUT *AUTL	<p>Команда Печать частных прав доступа для объектов *AUTL позволяет напечатать сведения о всех имеющихся в системах списках прав доступа. Для каждого списка в отчете указываются пользователи, у которых есть права доступа к нему, и сами права доступа. Эта информация полезна при анализе источников прав доступа к объектам вашей системы.</p> <p>Возможны три варианта вывода этого отчета. Полный отчет включает все списки прав доступа. В отчете об изменениях перечислены все изменения и добавления, внесенные с момента предыдущей обработки этого отчета. В отчете об удалениях перечислены пользователи, чьи права доступа к спискам прав доступа были удалены после предыдущей обработки этого отчета.</p> <p>При печати полного отчета вы можете выбрать печать списка объектов, защищенных списком прав доступа. Для каждого списка прав доступа система создаст отдельный отчет.</p>	QSECATLOLD ²
6, 45	PRTCMNSEC	<p>Команда Печать параметров защиты средств связи служит для печати параметров защиты системных объектов, имеющих отношение к средствам связи. Эти параметры определяют возможности доступа пользователей и заданий к вашей системе.</p> <p>Эта команда создает два отчета: в первом перечислены параметры списков конфигурации системы, а во втором - параметры защиты для описаний линий связи, контроллеров и описаний устройств. Для каждого отчета можно создать полную версию или версию со списком изменений.</p>	QSECCMNOLD ²
15, 54	PRTJOBDAUT	<p>Команда Печать информацию о правах доступа к описаниям заданий служит для печати списка описаний заданий, в которых указан пользовательский профайл и для которых заданы общие права доступа, отличные от *EXCLUDE. В отчете перечислены также специальные права доступа выбранного пользовательского профайла.</p> <p>Возможны два варианта вывода этого отчета. Полный отчет включает список всех описаний заданий, отвечающих заданным критериям выбора. В отчете об изменениях перечислены различия между описаниями заданий, находящимися в системе в настоящий момент, и описаниями, которые находились в системе в момент предыдущей обработки этого отчета.</p>	QSECJBDOLD ²

Таблица 238. Команды работы с отчетами о защите (продолжение)

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
См. примечание 4	PRTPUBAUT	<p>С помощью команды Печать объектов с общими правами доступа можно напечатать список объектов, общие права доступа к которым отличны от *EXCLUDE. При вызове команды необходимо указать тип объекта и одну или несколько библиотек. Команда PRTPUBAUT позволяет напечатать информацию об объектах, доступ к которым есть у различных пользователей системы.</p> <p>Возможны два варианта вывода этого отчета. Полный отчет включает список всех объектов, отвечающих критериям выбора. В отчете об изменениях перечислены различия между указанными объектами, находящимися в системе в настоящий момент, и объектами (того же типа и в той же библиотеке), которые находились в системе в момент предыдущей обработки этого отчета.</p>	QPВxxxxxx ⁵
См. примечание 4.	PRTPVTAUT	<p>Команда Печать частных прав доступа позволяет напечатать список частных прав доступа к объектам указанного типа в указанной библиотеке. С помощью этого отчета вы можете определить источники прав доступа к объектам.</p> <p>Возможны три варианта вывода этого отчета. Полный отчет включает список всех объектов, отвечающих критериям выбора. В отчете об изменениях перечислены различия между указанными объектами, находящимися в системе в настоящий момент, и объектами (того же типа и в той же библиотеке), которые находились в системе в момент предыдущей обработки этого отчета. В отчете об удалениях перечислены пользователи, чьи права доступа к каким-либо объектам были удалены после предыдущей обработки этого отчета.</p>	QPVxxxxxx ⁵
24, 63	PRTQAUT	<p>С помощью команды Печать прав доступа очереди можно напечатать параметры защиты для имеющихся в системе очередей ввода и очередей заданий. Эти параметры определяют пользователей, которые могут просматривать и изменять записи в очередях.</p> <p>Возможны два варианта вывода этого отчета. Полный отчет включает список всех объектов очередей вывода и очередей заданий, отвечающих критериям выбора. В отчете об изменениях перечислены различия между очередями вывода и очередями заданий, находящимися в системе в настоящий момент, и очередями, которые находились в системе в момент предыдущей обработки этого отчета.</p>	QSECQOLD ²

Таблица 238. Команды работы с отчетами о защите (продолжение)

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
25, 64	PRTSBSDAUT	<p>С помощью команды Печать описания подсистемы можно напечатать имеющиеся отношение к защите параметры связи для описаний подсистем. Эти параметры определяют способы поступления информации в систему и особенности выполнения заданий. Описание подсистемы включается в отчет только в том случае, если в нем содержатся записи средств связи, задающие имя пользовательского профайла.</p> <p>Возможны два варианта вывода этого отчета. Полный отчет включает список всех описаний подсистем, отвечающих критериям выбора. В отчете об изменениях перечислены различия между описаниями подсистем, находящимися в системе в настоящий момент, и объектами, которые находились в системе в момент предыдущей обработки этого отчета.</p>	QSECSBDOLD ²
26, 65	PRTSYSSECA	<p>Команда Печать системных атрибутов защиты служит для печати списка системных значений и сетевых атрибутов, влияющих на защиту. В отчете указано текущее и рекомендуемое значение.</p>	
27, 66	PRTRGPGM	<p>С помощью команды Печать программ триггеров можно напечатать список программ триггеров, связанных с файлами базы данных.</p> <p>Возможны два варианта вывода этого отчета. В полном отчете перечислены все присвоенные программы триггеров, отвечающие критериям выбора. В отчете об изменениях перечислены программы триггеров, которые были присвоены с момента последней обработки этого отчета.</p>	QSECTRGOLD ²
28, 67	PRTUSROBJ	<p>Команда Печать пользовательских объектов позволяет напечатать список пользовательских объектов (объектов, не поставляемых IBM), находящихся в заданной библиотеке. Этот отчет может пригодиться для печати списка пользовательских объектов, находящихся в какой-либо библиотеке (например, QSYS) из списка системных библиотек.</p> <p>Возможны два варианта вывода этого отчета. Полный отчет включает список всех пользовательских объектов, отвечающих критериям выбора. В отчете об изменениях перечислены различия между пользовательскими объектами, находящимися в системе в настоящий момент, и объектами, которые находились в системе в момент предыдущей обработки этого отчета.</p>	QSECPUOLD ²

Таблица 238. Команды работы с отчетами о защите (продолжение)

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
29, 68	PRTUSRPRF	Команда Печать пользовательского профайла служит для анализа пользовательских профайлов, отвечающих указанным критериям. Можно выбрать пользовательские профайлы по специальным правам доступа, по классу пользователя или по различию между этими параметрами. Вы можете напечатать информацию о правах доступа, среде или пароле.	
30, 69	PRTPRFINT	С помощью команды Печать внутренних объектов профайла вы можете напечатать отчет со сведениями о внутренних записях объекта пользовательского профайла (*USRPRF).	
31, 70	CHKOBJITG	С помощью команды Проверить целостность объекта можно определить, были ли рабочие объекты (например, программы) изменены без использования компилятора. Эта команда позволяет выявить попытки внедрения в систему вируса или попытки несанкционированного изменения программ.	
<p>¹ Опции меню SECBATCH.</p> <p>² Файл находится в библиотеке QUSRSYS.</p> <p>³ xx - это тип записи журнала, длиной в два символа. Например, файл вывода для записей журнала типа AE будет выглядеть как QSYS/QASYAEJ5. Модели файлов вывода описаны в Приложение F, "Макет записей журнала контроля", на стр. 593 данной книги.</p> <p>⁴ Меню SECTOOLS включает опции для выбора типов объектов, с которыми обычно работают администраторы защиты. Например, опция 11 или 50 позволяет запустить команду PRTPUBAUT для объектов *FILE. Задать тип объекта можно с помощью общих опций (18 и 57). Опции 12 и 51 запускают команду PRTPVTAUT для объектов *FILE. Задать тип объекта можно с помощью общих опций (19 и 58).</p> <p>⁵ Символы xxxxxx в имени файла обозначают тип объекта. Например, файл для программных объектов называется QBPBGM для общих прав доступа и QPVPGM - для частных прав доступа. Этот файл хранится в библиотеке QUSRSYS.</p> <p>В нем есть элементы, соответствующие каждой библиотеке, для которой вы создавали отчет. Имя элемента совпадает с именем библиотеки.</p> <p>⁶ Команда DSPAUDJRNE поддерживает не все типы записей контроля и показывает не все поля поддерживаемых записей.</p>			

Команды для тонкой настройки защиты

В этой таблице описаны команды, предназначенные для настройки защиты системы, содержащиеся в меню SECTOOLS.

Таблица 239. Команды для тонкой настройки защиты

Опция меню ¹	Команда	Описание	Применяемый файл базы данных
60	CFGSYSSEC	Команда Настроить защиту системы позволяет изменить системные значения защиты в связи с рекомендациями. Эта команда задает также параметры контроля действий. В разделе “Значения, устанавливаемые командой Настроить защиту системы” приведено описание выполняемых командой операций.	
61	RVKPUBAUT	С помощью команды Аннулировать общие права доступа можно задать для набора команд, требующих защиты, общие права доступа *EXCLUDE. В разделе “Команда Аннулировать общие права доступа” на стр. 761 приведено описание выполняемых командой операций.	
¹ Опции меню SECTOOLS.			

Значения, устанавливаемые командой Настроить защиту системы

В этой таблице перечислены системные значения, устанавливаемые при выполнении команды Настроить защиту системы (CFGSYSSEC), вызывающей программу QSYS/QSECCFGS.

Таблица 240. Значения, устанавливаемые командой CFGSYSSEC

Системное значение	Присваиваемое значение	Описание системного значения
QAUTOCFG	0 (Нет)	Автоматическая настройка новых устройств
QAUTOVRT	0	Число описаний виртуальных устройств, создаваемых системой при отсутствии доступных устройств.
QALWOBJRST	*NONE	Возможность восстановления программ режима системы и программ, принимающих права доступа
QDEVRCYACN	*DSCMSG (Отправлять сообщение при отключении)	Действие системы при восстановлении соединения
QDSCJOBITV	120	Интервал времени перед выполнением действия над отключенным заданием
QDSPSGNINF	1 (Да)	Определяет, нужно ли показывать пользователям информацию о входе в систему
QINACTITV	60	Интервал времени перед выполнением действия над интерактивным заданием
QINACTMSGQ	*ENDJOB	Действие, выполняемое системой над неактивным заданием
QLMTDEVSSN	1 (Да)	Запретить ли пользователям вход в систему с нескольких устройств одновременно
QLMTSECOFR	1 (Да)	Ограничить ли доступ к устройствам пользователей с правами *ALLOBJ и *SERVICE
QMAXSIGN	3	Максимальное число последовательных неудачных попыток входа в систему.
QMAXSGNACN	3 (Отключать и то, и другое)	Отключать ли рабочую станцию или пользовательский профайл при достижении максимального значения, указанного в QMAXSIGN.
QPWDEXPITV	60	Периодичность изменения паролей пользователей.

Таблица 240. Значения, устанавливаемые командой CFGSYSSEC (продолжение)

Системное значение	Присваиваемое значение	Описание системного значения
QPWDMINLEN	6 (см. прим. 3 и 5)	Минимальная длина пароля.
QPWDMAXLEN	8 (см. прим. 4 и 5)	Максимальная длина пароля.
QPWDPOSDIF	1 (Да) (см. прим. 5)	Должны ли различаться символы нового и старого пароля, стоящие в одних и тех же позициях.
QPWDLMTCHR	См. прим. 2 и 5	Символы, которые нельзя применять в пароле.
QPWDLMTAJC	1 (Да) (см. прим. 5)	Запрещать использование в паролях цифр в соседних позициях
QPWDLMTREP	2 (Запретить использование одинаковых символов в соседних позициях) (см. прим. 5)	Запретить использование в пароле одинаковых символов
QPWDRQDDGT	1 (Да) (см. прим. 5)	Пароль должен содержать хотя бы одну цифру
QPWDRQDDIF	1 (32 уникальных пароля)	Каждый раз при смене пароля пользователь должен задавать новый пароль. Использовать какой-либо старый пароль можно только при 33-й смене пароля.
QPWDRULES	<ul style="list-style-type: none"> • *MINLEN6 • *MAXLEN10 • *LMTSAMPOS • *LMTPRFNAME • *DGTMIN1 • *CHRLMTAJC • *DGTLMTAJC • *DGTLMTFST • *DGTLMTLST • *SPCCHRLMTAJC • *SPCCHRLMTFST • *SPCCHRLMTLST (см. прим. 6)	Правила для пароля.
QPWDVLDPGM	*NONE	Пользовательская программа выхода, вызываемая системой для проверки паролей.
QRMTSIGN	*FRCSIGNON	Способ управления запросами на вход в систему (удаленный вход или TELNET).
QRMTSVRATR	0 (Выключен)	Включен ли удаленный анализ неполадок в системе.
QSECURITY	50	Устанавливаемый уровень защиты.
QVFYOBJRST	3	Проверять восстанавливаемые объекты
Notes:		
1. Если текущее значение QSECURITY меньше или равно 30, то перед установкой более высокого уровня защиты прочитайте раздел Глава 2, “Работа с системным значением Защита системы (QSecurity)”, на стр. 9. 2. Набор запрещенных символов указан в сообщении с идентификатором CPXB302 в файле сообщений QSYS/QCPFMSG. Значение по умолчанию - AEIOU@\$. Для изменения набора запрещенных символов вызовите команду CHGMSGD (Изменить описание сообщения). 3. Если минимальная длина паролей уже больше 6, то системное значение QPWDMINLEN останется прежним. 4. Если максимальная длина паролей уже больше 8, то системное значение QPWDMAXLEN останется прежним. 5. Это системное значение изменяется только в том случае, если системное значение QPWDRULES равно *PWDSYSVAL. 6. Это системное значение не изменяется, если его значение равно *PWDSYSVAL.		

Кроме того, команда CFGSYSSEC устанавливает пустой пароль (*NONE) для следующих пользовательских профайлов, поставляемых IBM:

- QSYSOPR
- QPGMR
- QUSER
- QSRV
- QSRVBAS

И, наконец, команда CFGSYSSEC включает режим контроля в соответствии со значениями, указанными в команде CHGSECAUD (Изменить контроль действий).

Изменение программы

Если некоторые системные значения не соответствуют вашей среде, то вы можете создать свою собственную программу, запускаемую при вводе команды Настроить защиту системы (CFGSYSSEC).

Для изменения программы выполните следующие действия:

1. С помощью команды Получить исходный код на CL (RTVCLSRC) скопируйте исходный текст программы, которая запускается при вводе команды CFGSYSSEC. Это программа QSYS/QSECCFGS. Присвойте копии другое имя.
2. Внесите в текст программы необходимые изменения. Откомпилируйте ее. Помните: Важно случайно не удалить стандартную программу IBM QSYS/QSECCFGS. Для этого у вашей программы должно быть другое имя.
3. С помощью команды Изменить команду (CHGCMD) измените значение параметра PGM команды CFGSYSSEC. Укажите в качестве PGM имя своей программы. Например, если вы создали программу MYSECCFG в библиотеке QGPL, введите следующую команду:
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)

Notes:

- a. После изменения программы QSYS/QSECCFGS IBM не может гарантировать ее надежность, возможность обслуживания, уровень производительности и пригодность для какой-либо конкретной цели. При этом не гарантируется ее коммерческая ценность и пригодность для какой-либо конкретной цели.
- b. Если с командой RVKPUBAUT связана другая программа, запускаемая при вводе команды, то цифровая подпись этой команды станет недействительной.

Команда Аннулировать общие права доступа

Команда Аннулировать общие права доступа (RVKPUBAUT) позволяет установить для набора команд или программ общие права доступа *EXCLUDE.

Она запускает программу QSYS/QSECRVKP. Стандартная программа QSECRVKP аннулирует общие права доступа (устанавливая значение *EXCLUDE) для команд и интерфейсов прикладных программ (API), перечисленных в таблицах Табл. 241 на стр. 762 и Табл. 242 на стр. 762, соответственно. В новой системе команд и API заданы общие права доступа *USE.

Команды и интерфейсы, перечисленные в таблицах Табл. 241 на стр. 762 и Табл. 242 на стр. 762, потенциально могут нарушить нормальную работу системы. Администратор защиты должен явно предоставить права на запуск команд и программ тем пользователям, которым они действительно необходимы, запретив доступ всем остальным пользователям.

При вызове команды RVKPUBAUT задается библиотека, в которой хранятся команды. По умолчанию применяется библиотека QSYS. Если в вашей системе установлено несколько национальных языков, то эту команду необходимо вызвать для всех библиотек QSYSxxx.

Таблица 241. Команды, общие права доступа к которым устанавливаются командой RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

Все API, перечисленные в таблице Табл. 242, находятся в библиотеке QSYS:

Таблица 242. Программы, общие права доступа к которым устанавливаются командой RVKPUBAUT

QTIENDSUP		
QTISTRSUP		
QWTCTLTR		
QWTSETTR		
QY2FTML		

В V3R7 при выполнении команды RVKPUBAUT для корневого каталога устанавливаются общие права доступа *USE (если для него еще не установлены права доступа *USE или более низкие).

Изменение программы

Если некоторые значения не соответствуют вашей среде, то вы можете создать свою собственную программу, запускаемую при вводе команды Аннулировать общие права доступа (RVKPUBAUT).

Для изменения программы выполните следующие действия:

1. С помощью команды Получить исходный код на CL (RTVCLSRC) скопируйте исходный текст программы, которая запускается при вводе команды RVKPUBAUT. Это программа QSYS/QSECRVKP. Присвойте копии *другое имя*.
2. Внесите в текст программы необходимые изменения. Откомпилируйте ее. При этом важно случайно *не удалить* стандартную программу IBM QSYS/QSECRVKP. Для этого у вашей программы должно быть другое имя.
3. С помощью команды Изменить команду (CHGCMD) измените значение параметра PGM команды RVKPUBAUT. Укажите в качестве PGM имя своей программы. Например, если вы создали программу MYRVKPGM в библиотеке QGPL, введите следующую команду:
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)

Notes:




- а. После изменения программы QSYS/QSECRVKP IBM не может гарантировать ее надежность, возможность обслуживания, уровень производительности и пригодность для какой-либо конкретной цели. При этом не гарантируется ее коммерческая ценность и пригодность для какой-либо конкретной цели.

- b. Если с командой RVJPUDAUT связана другая программа, запускаемая при вводе команды, то цифровая подпись этой команды станет недействительной.


Приложение Н. Связанная информация для справочника по защите i5/OS


Здесь приведены описания продуктов и руководства IBM Redbooks (в формате PDF), web-сайты и разделы справочной системы Information Center, относящиеся к защите. Вы можете просмотреть или напечатать любой из документов в формате PDF.

Руководства


- Публикация Восстановление системы (примерно 8.42 Мб) содержит сведения по вопросам планирования стратегии резервного копирования и восстановления, информацию о процедурах сохранения и восстановления информации в системе, а также описание пулов вспомогательной памяти и вариантов защиты дисковых накопителей.
- Публикация Установка, обновление и удаление i5/OS и связанного программного обеспечения (3053 Кб) содержит пошаговые инструкции по установке системы, лицензионных программ, временных исправлений программ (PTF), а также поддержки дополнительных языков, поставляемой IBM.
- Публикация Поддержка удаленных рабочих станций  (1636 Кб) содержит сведения о настройке и применении функций поддержки удаленных рабочих станций, таких как удаленный вход в систему дисплейной станции, распределенные средства работы с командами хоста и удаленное подключение 3270.
- В публикации Cryptographic Support/400  (448 Кб) описаны функции защиты данных лицензионного программного продукта Cryptographic Facility. Она содержит рекомендации по работе с этим продуктом и справочную информацию для программистов.
- В публикации Настройка локальных устройств  (763 Кб) приведена информация о начальной настройке системы и изменении ее конфигурации. Кроме того, в ней приведены общие сведения о настройке устройств.
- В публикации *SNA Distribution Services*, SC41-5410 (2259 Кб) приведена информация о настройке служб рассылки системной сетевой архитектуры (SNADS) и моста VM/MVS в сети. Кроме того, она содержит сведения о функциях рассылки объектов, службах библиотеки документов и службах системного каталога рассылки. Это руководство не включено в данный выпуск i5/OS Information Center. Однако оно может быть полезным. Это руководство можно заказать в IBM Publications Center в виде книги или бесплатной электронной публикации.
- Публикация *ADTS for AS/400: Source Entry Utility*, SC09-2605 (460 Кб) содержит информацию о создании и изменении элементов исходных файлов с помощью Утилиты ввода исходного кода (SEU), входящей в состав средств разработки приложений. В книге описаны процедуры запуска и завершения сеансов SEU, а также приведены инструкции по применению различных функций этого полноэкранный текстового редактора. Книга содержит примеры выполнения различных задач, начиная от использования простых команд до применения заранее созданных приглашений на языках высокого уровня и форматов данных. Эти примеры рассчитаны на пользователей с различным уровнем подготовки. Это руководство не включено в данный выпуск i5/OS Information Center. Однако оно может быть полезным. Это руководство можно заказать в IBM Publications Center в виде книги или бесплатной электронной публикации.

Руководства по выполнению задач IBM

- Публикация IBM Redbook AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet  (2.1 Мб) содержит сведения о различных вопросах защиты, в том числе о возможных негативных последствиях подключения системы System i к Internet. В ней приведены примеры, рекомендации, советы и методики, применяемые при разработке приложений.

- Публикация IBM Redbook Cool Title About the AS/400 and Internet  (7.36 Мб) содержит информацию, которая поможет вам понять принципы работы с сетью Internet (или внутренней сетью) в системе System i и применить эти принципы на практике. Она содержит сведения о применении различных функций системы. С ее помощью можно быстро начать работу с электронной почтой, функциями передачи файлов, эмуляцией терминалов, протоколами gohper и HTTP, а также шлюзом между 5250 и HTML.

Сайты в Internet

- Lotus Documentation  (<http://www-10.lotus.com/ldd/doc>)
 Данный Web-сайт содержит информацию о Lotus Notes, Domino и IBM Domino для i5/OS. С этого Web-сайта можно загрузить информацию в формате базы данных Domino (.NSF) или Adobe Acrobat (.PDF), выполнить поиск в базе данных и найти сведения о получении отпечатанной версии руководств.

Прочая информация

- В публикации Планирование и настройка защиты системы приведена подборка практических рекомендаций по применению функций защиты iSeries и организации работы в соответствии с требованиями к защите. Дополнительно приведена информация о настройке и применении функций защиты, входящих в состав i5/OS.
- *Implementing AS/400 Security, 4th Edition* (October 15, 2000) by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press. Здесь приведены инструкции и практические советы по планированию, настройке и управлению защитой системы.

Номер ISBN

1583040730

- Публикация System i Access for Windows содержит техническую информацию о программах System i Access for Windows для всех версий System i Access for Windows
- Раздел Настройка TCP/IP содержит сведения о настройке и работе с TCP/IP.
- В разделе Приложения TCP/IP, протоколы и службы приведена информация о работе с приложениями TCP/IP, такими как FTP, SMTP и TELNET.
- Раздел Работа с системой содержит информацию о запуске и завершении работы системы и устранении неполадок.
- Раздел Интегрированная файловая система содержит обзор интегрированной файловой системы, включающий ее описание, способы применения и доступные интерфейсы.
- Публикация iSeries и защита в Internet поможет правильно настроить защиту системы при подключении iSeries к Internet. Дополнительная информация приведена на домашней странице IBM I/T (Information Technology) Security: <http://www.ibm.com/security>. Раздел Оптическая память содержит описание функций работы с *оптическими устройствами*. Приведены сведения о применении устройств чтения компакт-дисков, а также библиотек оптических носителей, подключенных напрямую или по сети.
- Раздел Печать содержит общую информацию о печати, описание файлов принтера и функции поддержки буферизации вывода на принтер, а также сведения о подключении принтеров.
- Публикация Язык CL содержит различные сведения о разработке программ, в том числе общую информацию об объектах и библиотеках, программировании на языке CL, управлении потоком и обмене данными между программами, работе с объектами в программах на CL и создании программ на CL. В других разделах приведена информация о заранее подготовленных и динамически составляемых сообщениях, обработке сообщений, определении и создании пользовательских команд и меню и тестировании приложений с использованием режима отладки, точек прерывания, трассировки и функций просмотра.
 Также приведено полное описание языка CL iSeries и команд i5/OS. Команды i5/OS служат для вызова функций лицензионной программы i5/OS (5722-SS1). Все команды, не входящие в состав CL i5/OS, связаны с другими лицензионными программами, в том числе различными языками и утилитами. Они описаны в публикациях по соответствующим лицензионным программам.
- Раздел Программирование содержит информацию о многих языках программирования и утилитах iSeries. В том числе, он содержит общие сведения по следующим вопросам:

- Сведения о всех командах CL iSeries (в программах i5/OS и других лицензионных программах) в различных форматах.
- Информацию, связанную с командами CL, такую как сообщения об ошибках, которые можно отслеживать для каждой команды, и поставляемые IBM файлы, которые используются некоторыми командами.
- Сведения о поставляемых IBM объектах, в том числе библиотеках.
- Сведения о поставляемых IBM системных значениях.
- Ключевые слова DDS для физических и логических файлов, файлов принтера и дисплея, а также файлов ICF.
- Инструкции REXX и встроенные функции.
- Сведения о других языках программирования (таких как RPG) и утилитах (таких как SEU и SDA).
- В разделе Управление системами приведена информация о сборе статистических данных, изменении системных значений и управлении памятью системы.
- Раздел Концепции файлов базы данных содержит общие сведения о разработке, создании, запуске и тестировании операторов DB2 Query Manager и SQL Development Kit для i5/OS. В нем также описан язык структурных запросов (SQL) и приведены примеры применения операторов SQL в программах на языках COBOL, RPG, C, FORTRAN и PL/I. Также в нем содержится следующая информация:
 - Создание, сохранение и запуск запросов SQL
 - Создание простых и сложных отчетов
 - Создание, обновление, управление, отправка запросов и создание отчетов для таблиц базы данных с помощью интерфейса форм
 - Определение запросов SQL и отчетов и создание их прототипов для использования в прикладных программах

Сохранение PDF-файлов

Для сохранения файла PDF на рабочей станции с целью его последующего просмотра или печати выполните следующие действия:

1. Щелкните правой кнопкой мыши на приведенной выше ссылке.
2. Выберите пункт, позволяющий сохранить PDF на локальном компьютере.
3. Откройте каталог, в котором следует сохранить документ PDF.
4. Нажмите кнопку **Сохранить**.

Загрузка Acrobat Reader

Для просмотра и печати файлов PDF необходима программа Adobe Reader. Бесплатную копию этой программы можно загрузить с Web-сайта Adobe по адресу Adobe Web site

(www.adobe.com/products/acrobat/readstep.html)  .

Приложение I. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM не распространяет продукты, службы и компоненты, описанные в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM может обладать патентами или заявками на получение патента по отношению к материалам, упоминаемым в настоящем документе. Предоставление настоящего документа не означает предоставления каких-либо лицензий на патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM
Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или (в письменном виде) по следующему адресу:

IBM World Trade Asia Corporation
Лицензирование
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также другим странам, в которых это заявление противоречит местному законодательству: ФИРМА INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отрицать предоставление каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому указанное заявление может не иметь места в вашем случае.

В данной публикации могут содержаться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены в последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью документации по данному продукту IBM, и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этой информации лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM, Соглашения о лицензии на машинный код или любого другого эквивалентного соглашения.

Данные о быстродействии, приведенные в документах, были получены на системах, настроенных особым образом. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли выполняться в системах, находящихся на этапе разработки. В системах, поставляемых заказчикам, результаты измерений могут быть другими. Более того, некоторые значения могли быть получены в результате экстраполяции. Фактические результаты могут различаться. Пользователи, работающие с настоящим документом, должны оценить степень применимости данных к своей среде.

Информация о продуктах других фирм была получена от поставщиков этих продуктов, из опубликованных ими документов или других общедоступных источников. Эти продукты не были проверены IBM. Точность приводимых данных о быстродействии, совместимости и других сведений о продуктах, выпущенных сторонними компаниями, не гарантируется. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления о будущих намерениях и планах фирмы IBM приведены только для общего сведения. Фирма IBM оставляет за собой право отказываться от этих заявлений и вносить в них изменения без дополнительного предупреждения.

Все приведенные цены IBM являются текущими рекомендованными розничными ценами IBM и могут быть изменены без предварительного уведомления. Цены дилеров могут быть другими.

Данная информация носит предварительный характер и предназначена только для планирования. Информация может измениться до того, как описанные в ней продукты станут доступными.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для максимальной достоверности в них приведены имена отдельных лиц, названия компаний, товарных знаков и продуктов. Все эти имена и названия вымышлены, и любое их сходство с реальными именами, названиями и адресами носит совершенно случайный характер.

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ:

Данная документация содержит примеры исходного текста программы, иллюстрирующие различные приемы программирования для различных платформ. Вы можете копировать, видоизменять и распространять эти примеры программ в любом виде без возникновения каких-либо денежных обязательств перед IBM с целью разработки, применения, продажи или распространения прикладных программ, соответствующих стандартам интерфейсов прикладного программирования для той платформы, для которой написаны эти примеры программ. Работа примеров не была проверена во всех возможных условиях. Поэтому IBM не может гарантировать или подразумевать надежность, пригодность и функциональность этих программ.

Каждая копия или любая часть этих примеров программ или программ, построенных на их основе, должна включать в себя следующую информацию об авторских правах:

© (название вашей компании) (год). Этот код разработан на основе примеров кода фирмы IBM в составе примеров программ. © Авторские права принадлежат IBM Corp. _год или годы_. Все авторские права сохранены.

Если данный документ представлен в электронном виде, в нем могут отсутствовать фотографии и цветные иллюстрации.

Сведения о программных интерфейсах

Эта публикация о защите документирует рекомендуемые интерфейсы программирования, позволяющие создавать программы, использующие службы i5/OS.

Товарные знаки

Ниже перечислены товарные знаки фирмы International Business Machines Corporation, зарегистрированные в США и/или других странах:

AIX
i5/OSIBMIBM (logo)
System i
z/OS

Intel, Intel Inside (logos), MMX, и Pentium являются товарными знаками фирмы Intel Corporation в США и других странах.

Microsoft, Windows, Windows NT и логотип Windows - это товарные знаки Microsoft Corporation в США и/или других странах.

Java и все товарные знаки на основе Java являются товарными знаками Sun Microsystems, Inc. в США и/или других странах.

Linux является зарегистрированным товарным знаком Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

UNIX - это зарегистрированный товарный знак The Open Group в США и/или других странах.

Названия других фирм, продуктов и услуг могут быть товарными или служебными знаками других компаний.

Windows

Условия и соглашения

Разрешение на использование этих публикаций предоставляется в соответствии с следующими условиями и соглашениями.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные

публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если по мнению IBM использование этих публикаций может принести ущерб интересам IBM или если IBM будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях "как есть", без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, отсутствия нарушений или применения для каких-либо конкретных целей.

Индекс

Спец. символы

(*Mgt), права на управление 138
(*Ref), права на обращение 138
(Переместить), команда

необходимые права доступа к объектам 425

(Показать ссылку), команда

необходимые права доступа к объектам 421

*ADD (добавление), права доступа 138, 360

*ADOPTED (принятые), права доступа 163

*ADVANCED (расширенный), уровень поддержки 85

*ALL (все), права доступа 140, 361

*ALLOBJ

права доступа класса пользователей 10

*ALLOBJ (ко всем объектам), специальные права доступа

добавлено системой

изменение уровня защиты 13

неудачный вход в систему 211

параметров контроля 274

разрешенные функции 90

риски 90

удаление системой

восстановление профайла 263

изменение уровня защиты 13

*ALRTBL (таблица предупреждений), контроль за объектом 531

*ASSIST, программа обработки клавиши Attention 110

*AUDIT (контроль), специальные права доступа

разрешенные функции 93

риски 93

*AUTFAIL (ошибка прав доступа), уровень контроля 286

*AUTHLR (владелец прав доступа), контроль за объектом 532

*AUTL (список прав доступа), контроль за объектом 531

*AUTLMGT (управление списком прав доступа), права доступа 138, 360

*BASIC (основной), уровень поддержки 85

*BNDDIR (каталог связывания), контроль за объектом 532

*BREAK (прерывать), режим доставки пользовательский профайл 107

*CFGL (список конфигурации), контроль за объектом 533

*CHANGE (изменение), права доступа 140, 361

*CHRSF (особые файлы), контроль за объектом 533

*CHTFMT (формат диаграммы), контроль за объектом 533

*CLD (описание локали C), контроль за объектом 534

*CLKWD (ключевое слово CL), опция пользователя 112, 113, 114

*CLS (класс), контроль за объектом 535

*CMD (команда), контроль за объектом 535

*CMD (текст команды), уровень контроля 288

*CNL (список соединений), контроль за объектом 536

*COSD (класс обслуживания), контроль за объектом 537

*CREATE (создание), уровень контроля 288

*CRQD

восстановление

запись журнала контроля

(QAUDJRN) 293

*CRQD (описание запроса на изменение), контроль за объектом 534

*CSI (исходная информация связи), контроль за объектом 537

*CSPMAP (список межсистемных продуктов), контроль за объектом 537

*CSPTBL (таблица межсистемных продуктов), контроль за объектом 538

*CTLD (описание контроллера), контроль за объектом 538

*DELETE (удаление), уровень контроля 288

*DEVD (описание устройства), контроль за объектом 539

*DFT (по умолчанию), режим доставки пользовательский профайл 107

*DIR (каталог), контроль за объектом 540

*DISABLED (отключен), состояние пользовательского профайла

QSECOFR (пользовательский профайл

системного администратора) 83

описание 83

*DLT (удаление), права доступа 138, 360

*DOC (документ), контроль за объектом 544

*DTAARA (область данных), контроль за объектом 547

*DTADCT (словарь данных), контроль за объектом 548

*DTAQ (очередь данных), контроль за объектом 548

*EDTD (описание формата), контроль за объектом 549

*ENABLED (включен), состояние пользовательского профайла 83

*EXCLUDE (запретить), права доступа 140

*EXECUTE (выполнение), права доступа 138, 360

*EXITRG (запись регистрации точки выхода), контроль за объектом 549

*EXPERT (эксперт), опция

пользователя 112, 113, 114, 167

*FCT (таблица управления формами), контроль за объектом 550

*FILE (файл), контроль за объектом 550

*FNTRSC (ресурс шрифта), контроль за объектом 554

*FORMDF (определение формы), контроль за объектом 554

*FTR (фильтр), контроль за объектом 554

*GROUP (группа), права доступа 163

*GSS (набор графических символов), контроль за объектом 555

*HLPFULL (полноэкранная справка), опция пользователя 114

*HOLD (блокировать), режим доставки пользовательский профайл 107

*IGCDCT (словарь набора двухбайтовых символов), контроль за объектом 556

*IGCSRT (сортировка набора двухбайтовых символов), контроль за объектом 556

*IGCTBL (таблица набора двухбайтовых символов), контроль за объектом 556

*INTERMED (промежуточный), уровень поддержки 85

*IOSYSCFG (конфигурация системы), специальные права доступа

разрешенные функции 94

риски 94

*JOBCTL (управление заданиями), специальные права доступа

ограничение приоритета

(PTYLMT) 100

очередь вывода, параметры 223

разрешенные функции 91

риски 91

*JOBDB (описание задания), контроль за объектом 557

*JOBDBA (изменение задания), уровень контроля 289

*JOBQ (очередь заданий), контроль за объектом 557

*JOBSCD (планировщик заданий), контроль за объектом 558

*JRN (журнал), контроль за объектом 559

*JRNRCV (получатель журнала), контроль за объектом 560

*LIB (библиотека), контроль за объектом 561

*LIND (описание линии), контроль за объектом 561

*MENU (меню), контроль за объектом 563

*Mgt (управление), права доступа 138

*MODD (описание режима), контроль за объектом 563

*MODULE (модуль), контроль за объектом 564

- *MSGF (файл сообщений), контроль за объектом 564
- *MSGQ (очередь сообщений), контроль за объектом 565
- *NODGRP (группа узлов), контроль за объектом 566
- *NODL (список узлов), контроль за объектом 566
- *NOSTSMMSG (сообщение об отсутствии состояния), опция пользователя 114
- *NOTIFY (уведомлять), режим доставки пользовательский профайл 107
- *NTBD (описание NetBIOS), контроль за объектом 567
- *NWID (сетевой интерфейс), контроль за объектом 567
- *NWSD (описание сетевого сервера), контроль за объектом 568
- *OBJALTER (изменение объекта), права доступа 138, 360
- *OBJEXIST (существование объекта), права доступа 138, 360
- *OBJMGT (управление объектом), значение 291
- *OBJMGT (управление объектом), права доступа 138, 360
- *OBJOPR (операционные права доступа к объекту) 138, 360
- *OBJREF (обращение к объекту), права доступа 138, 360
- *OFCSRV (функции Office), уровень контроля 291, 542, 562
- *OUTQ (очередь вывода), контроль за объектом 568
- *OVL (перекрытие), контроль за объектом 570
- *PAGDFN (определение страницы), контроль за объектом 570
- *PAGSEG (сегмент страницы), контроль за объектами 570
- *PARTIAL (неполное), ограничить возможности 88
- *PDG (группа дескрипторов печати), контроль за объектом 571
- *PGM (программа), объект 571
- *PGMADP (принятые права доступа), уровень контроля 292
- *PGMFAIL (сбой программы), уровень контроля 292
- *PNLGRP (группа панелей), контроль за объектом 572
- *PRDAVL (уровень готовности продукта), контроль за объектом 573
- *PRDDFN (определение продукта), контроль за объектом 573
- *PRDLOD (компоновка программных продуктов), контроль за объектом 573
- *PRTDTA (вывод на принтер), уровень контроля 293
- *PRTMSG (печать сообщения), опция пользователя 114
- *QMFORM (форма Query Manager), контроль за объектом 573
- *QMQRV (запрос Query Manager), контроль за объектом 574
- *QRYDFN (определение запроса), контроль над объектом 575
- *R (чтение) 140, 362
- *RCT (таблица информационных кодов), контроль за объектом 576
- *READ (чтение), права доступа 138, 360
- *Ref (обращение), права доступа 138
- *ROLLKEY (клавиша прокрутки), опция пользователя 114
- *RW (чтение, запись) 140, 362
- *RWX (чтение, запись, выполнение) 140, 362
- *RX (чтение, выполнение) 140, 362
- *S36 (описание системы S/36), контроль за объектом 587
- *SAVRST (сохранение/восстановление), уровень контроля 293
- *SAVSYS (специальные права на сохранение системы)
 - *OBJEXIST, права доступа 138, 360
 - описание 270
 - разрешенные функции 92
 - риски 92
 - удаление системой
 - изменение уровня защиты 13
- *SBSD (описание подсистемы), контроль за объектом 577
- *SCHIDX (индекс поиска), контроль за объектом 578
- *SECADM (администратор защиты), специальные права доступа 90
- разрешенные функции 90
- *SECURITY (защита), уровень контроля 297
- *SERVICE (сервисные средства), уровень контроля 301
- *SERVICE, специальные служебные права доступа
 - неудачный вход в систему 211
 - разрешенные функции 92
 - риски 92
- *SIGNOFF начальное меню 87
- *SOCKET (локальный сокет), контроль за объектом 578
- *SPADCT (орфографический словарь), контроль за объектом 580
- *SPLCTL (управление буфером), специальные права доступа
- очередь вывода, параметры 224
- разрешенные функции 91
- риски 91
- *SPLFDTA (изменения буферного файла), уровень контроля 301, 581
- *SQLPKG (пакет SQL), контроль за объектом 582
- *SRVPGM (служебная программа), контроль за объектом 583
- *SSND (описание сеанса), контроль за объектом 584
- *STMF (поточковый файл), контроль за объектом 584
- *STSMMSG (сообщение о состоянии), опция пользователя 114
- *SVRSTG (область памяти сервера), объект 584
- *SYNLNK (символьная ссылка), контроль за объектом 586
- *SYSMGT (управление системами), уровень контроля 301
- *SYSTEM (система), домен 16
- *SYSTEM (система), режим 16
- *TBL (таблица), контроль за объектом 588
- *TYPEAHEAD (буферизация ввода), буферизация клавиатуры 99
- *UPD (обновление), права доступа 138, 360
- *USE (использование), права доступа 140, 361
- *USER (пользователь), домен 16
- *USER (пользователь), режим 16
- *USRIDX (пользовательский индекс), контроль за объектом 588
- *USRIDX (пользовательский индекс), объект 20
- *USRPRF (пользовательский профайл), контроль за объектом 589
- *USRQ (пользовательская очередь), контроль за объектом 590
- *USRQ (пользовательская очередь), объект 20
- *USRSPC (пользовательское пространство), контроль за объектом 590
- *USRSPC (пользовательское пространство), объект 20
- *VLDL (контрольный список), контроль за объектом 590
- *W (запись) 140, 362
- *WX (запись, выполнение) 140, 362
- *X (выполнение) 140, 362
- >Система имен доменов (DNS)
 - права доступа к объектам, необходимые для применения команд 401

A

- access, команда (Определить доступные файлы)
 - контроля объекта 540
- accessx, команда (Определить доступные файлы)
 - контроля объекта 540
- ACGCDE (код учета ресурсов), параметр
 - изменение 105
 - пользовательский профайл 105
- AD (изменение контроля), тип записи журнала 297
- AD (изменение параметров контроля), формат файла 601
- ADDACC (Добавить код доступа), команда
 - контроля объекта 547
 - необходимые права доступа к объектам 476
- ADDAJE (Добавить запись автоматического задания), команда
 - контроля объекта 577
 - необходимые права доступа к объектам 510
- ADDALRACNE (Добавить запись о действии при получении предупреждения), команда
 - контроля объекта 554

ADDALRACNE (Добавить запись о действии при получении предупреждения), команда
(*продолжение*)
необходимые права доступа к объектам 411

ADDALRD (Добавить описание предупреждения), команда
контроля объекта 531
необходимые права доступа к объектам 373

ADDALRSLTE (Добавить запись о выборе предупреждений), команда
контроля объекта 554
необходимые права доступа к объектам 411

ADDAUTLE (Добавить запись в список прав доступа), команда
использование 175
контроля объекта 531
необходимые права доступа к объектам 375
описание 327

ADDBKP (Добавить точку прерывания), команда
необходимые права доступа к объектам 490

ADDBNDDIRE (Добавить запись каталога связывания), команда
контроля объекта 532
необходимые права доступа к объектам 376

ADDBSCDEVE (Добавить запись об устройстве BSC), команда
контроля объекта 551

ADDCFGLE (Добавить записи в список конфигурации), команда
контроля объекта 533
необходимые права доступа к объектам 385

ADDCMKMSFE, команда
необходимые права доступа к объектам 388

ADDCLUNODE, команда
необходимые права доступа к объектам 378
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDCMDCRQA (Добавить операцию запроса на изменение команды), команда
контроля объекта 534
необходимые права доступа к объектам 377
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDCMNDEVE (Добавить запись об устройстве средств связи), команда
контроля объекта 551

ADDCMNE (Добавить запись средств связи), команда
контроля объекта 577
необходимые права доступа к объектам 510

ADDCNNLE (Добавить запись списка соединений), команда
контроля объекта 536

ADDCOMSNMP (Добавить взаимодействие для SNMP), команда
необходимые права доступа к объектам 517

ADDCRGDEVE, команда
необходимые права доступа к объектам 379
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDCRGNODE, команда
необходимые права доступа к объектам 379
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDCRSDMNK (Добавить междоменный ключ шифрования ключа), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDDEVDMNE, команда
необходимые права доступа к объектам 379
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDDIRE (Добавить запись каталога), команда
необходимые права доступа к объектам 393
описание 333

ADDDIRSHD (Добавить теневой каталог), команда
необходимые права доступа к объектам 393

ADDLLOAUT (Добавить права доступа к объекту библиотеки документов), команда
контроля объекта 545
необходимые права доступа к объектам 396
описание 332

ADDDSPDEVE (Добавить запись о дисплеем устройстве), команда
контроля объекта 551

ADDDSTLE (Добавить запись в список рассылки), команда
необходимые права доступа к объектам 396

ADDDSTQ (Добавить очередь рассылки), команда
необходимые права доступа к объектам 395
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDDSTRTE (Добавить маршрут рассылки), команда
необходимые права доступа к объектам 395

ADDDSTRTE (Добавить маршрут рассылки), команда (*продолжение*)
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDDSTSYSN (Добавить альтернативное имя системы для рассылки), команда
необходимые права доступа к объектам 395
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDDTADFN (Добавить определение данных), команда
необходимые права доступа к объектам 435

ADDEMLCFGE (Добавить запись конфигурации эмуляции), команда
необходимые права доступа к объектам 392

ADDENVVAR (Добавить переменную среды), команда
необходимые права доступа к объектам 403

ADDEWCBCDE (Добавить запись штрихового кода для контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 403

ADDEWCM (Добавить элемент контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 403

ADDEWCPTCE (Добавить запись PTC контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 403

ADDEWLM (Добавить элемент линии расширенной беспроводной сети), команда
необходимые права доступа к объектам 403

ADDEXITPGM (Добавить программу выхода), команда
контроля объекта 549
необходимые права доступа к объектам 496
пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDFCTE (Добавить запись таблицы управления формам), команда
необходимые права доступа к объектам 498

ADDFNTTBLE (Добавить запись таблицы шрифтов DBCS)
права доступа к объектам,
необходимые для применения команд 372

ADDICFDEVE (Добавить запись об устройстве функции межсистемной связи), команда
контроля объекта 551

ADDICFDEVE (Добавить запись об устройстве функции межсистемной связи), команда *(продолжение)* необходимые права доступа к объектам 404

ADDIMGCLGE, команда необходимые права доступа к объектам 414

ADDIPSIFC (Добавить интерфейс IP для SNA), команда необходимые права доступа к объектам 373

ADDIPSLOC (Добавить запись о расположении IP для SNA), команда необходимые права доступа к объектам 373

ADDIPSRTE (Добавить маршрут IP для SNA), команда необходимые права доступа к объектам 373

ADDJOBQE (Добавить запись очереди заданий), команда контроля объекта 557, 577 необходимые права доступа к объектам 510

ADDJOBSCDE (Добавить запись расписания заданий), команда SECVATCH, меню 753 контроля объекта 558 необходимые права доступа к объектам 443

ADDLANADPI (Добавить информацию об адаптере LAN), команда необходимые права доступа к объектам 464

ADDLFM (Добавить элемент логического файла), команда контроля объекта 551 необходимые права доступа к объектам 404

ADDLIBLE (Добавить запись списка библиотек), команда 218, 221 необходимые права доступа к объектам 456

ADDLICKEY (Добавить ключ лицензии), команда необходимые права доступа к объектам 461

ADDLNK (Добавить ссылку), команда контроля объекта 579, 584 необходимые права доступа к объектам 415

ADDMMFS (Добавить смонтированную файловую систему), команда необходимые права доступа к объектам 472, 519 пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDMSGD (Добавить описание сообщения), команда контроля объекта 565 необходимые права доступа к объектам 467

ADDMSTPART, команда необходимые права доступа к объектам 388

ADDNETJOB (Добавить запись сетевого задания), команда необходимые права доступа к объектам 471 пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDNETTBLE (Добавить запись таблицы сетей), команда необходимые права доступа к объектам 517

ADDNODLE (Добавить запись списка узлов), команда контроля объекта 567 необходимые права доступа к объектам 475

ADDNWSSTGL (Подключить область памяти сетевого сервера), команда необходимые права доступа к объектам 473

ADDOBJCRQA (Добавить операцию запроса на изменение объекта), команда контроля объекта 534 необходимые права доступа к объектам 377 пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDOFCENR (Добавить регистрацию в Office), команда контроля объекта 545

ADDOPTCTG (Добавить оптическую кассету), команда необходимые права доступа к объектам 478 пользовательские профайлы, поставляемые IBM, с правами доступа 347

ADDOPTSVR (Добавить оптический сервер), команда необходимые права доступа к объектам 478 пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDPCCST (Добавить ограничение для физического файла), команда необходимые права доступа к объектам 404

ADDPXDFN (Добавить определение PEX), команда необходимые права доступа к объектам 482 пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDPXFT (Добавить фильтр PEX), команда необходимые права доступа к объектам 498 пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDPFCST (Добавить ограничение для физического файла), команда контроля объекта 551

ADDPFM (Добавить элемент физического файла), команда контроля объекта 551

ADDPFM (Добавить элемент физического файла), команда *(продолжение)* необходимые права доступа к объектам 404

ADDPFTRG (Добавить триггер для физического файла), команда контроля объекта 551 необходимые права доступа к объектам 404

ADDPFVLM (Добавить элемент переменной длины в физический файл), команда контроля объекта 551

ADDPGM (Добавить программу), команда необходимые права доступа к объектам 490

ADDPJE (Добавить запись предварительного задания), команда контроля объекта 577 необходимые права доступа к объектам 510

ADDPRBACNE (Добавить запись о действии в случае неполадки), команда контроля объекта 554 необходимые права доступа к объектам 411, 489

ADDPRBSLTE (Добавить запись о выборе неполадок), команда контроля объекта 555 необходимые права доступа к объектам 411, 489

ADDPDRCRQA (Добавить операцию запроса на изменение продукта), команда контроля объекта 534 необходимые права доступа к объектам 377 пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDPDLICI (Добавить информацию о лицензии на продукт), команда контроля объекта 573

ADDPDTCRQA (Добавить операцию запроса на изменение PTF), команда контроля объекта 534 необходимые права доступа к объектам 377 пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDRDBDIRE (Добавить запись каталога реляционной базы данных), команда необходимые права доступа к объектам 497

ADDRJECMNE (Добавить запись средств связи RJE), команда необходимые права доступа к объектам 498

ADDRJERDRE (Добавить запись программы чтения RJE), команда необходимые права доступа к объектам 498

ADDRJEWTR (Добавить запись программы записи RJE), команда необходимые права доступа к объектам 498

ADDRMTJRN (Добавить удаленный журнал), команда
контроль объекта 559

ADDRMTSVR (Добавить удаленный сервер), команда
необходимые права доступа к объектам 474

ADDRPYLE (Добавить запись списка ответов), команда
контроль объекта 576
необходимые права доступа к объектам 513
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDRSCCRQA (Добавить операцию запроса на изменение ресурса), команда
контроль объекта 534
необходимые права доступа к объектам 377
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDRTGE (Добавить запись о выполнении), команда
контроль объекта 577
необходимые права доступа к объектам 510

ADDSCHIDX (Добавить запись индекса поиска), команда
контроль объекта 572, 578
необходимые права доступа к объектам 436

ADDSOCE (Добавить запись сферы управления), команда
необходимые права доступа к объектам 507

ADDSRVTBLE (Добавить запись таблицы служб), команда
необходимые права доступа к объектам 517

ADDSVRAUTE (Добавить запись идентификации сервера), команда
необходимые права доступа к объектам 502

ADDTAPCTG (Добавить кассету магнитной ленты), команда
необходимые права доступа к объектам 464

ADDTCPRTE (Добавить запись таблицы хостов TCP/IP), команда
объект необходимые права доступа 517

ADDTCRIFC (Добавить интерфейс TCP/IP), команда
необходимые права доступа к объектам 517

ADDTCRPPORT (Добавить ограничение на порт TCP/IP), команда
необходимые права доступа к объектам 517

ADDTCRPSI (Добавить удаленную систему TCP/IP), команда
необходимые права доступа к объектам 517
объект, права доступа, необходимые 517

ADDTCPRTE (Добавить маршрут TCP/IP), команда
необходимые права доступа к объектам 517

ADDTRC (Добавить трассировку), команда
необходимые права доступа к объектам 490

ADDTRCFTR
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ADDWSE (Добавить запись рабочей станции), команда
контроль объекта 577
необходимые права доступа к объектам 511

ADSM (QADSM), пользовательский профайл 339

advanced function printing (AFP)
права доступа к объектам, необходимые для применения команд 372

AF (отсутствие необходимых прав доступа), формат файла 604

AF (ошибка прав доступа), тип записи журнала
запрещенная команда 19
нарушение аппаратной защиты 18
нарушение входа в систему по умолчанию 17
нарушение описания задания 17
неподдерживаемый интерфейс 17, 19
описание 286, 292
проверка программы 18, 19

AF_INET, сокет для SNA
права доступа к объектам, необходимые для применения команд 373

AFDFTUSR (QAFDFTUSR), пользовательский профайл 339

AFOWN (QAFOWN), пользовательский профайл 339

AFP (Advanced Function Printing)
права доступа к объектам, необходимые для применения команд 372

AFUSR (QAFUSR), пользовательский профайл 339

ALCOBJ (Захватить объект), команда
контроль объекта 529
необходимые права доступа к объектам 364

ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр
Изменить команду (CHGCMD), команда 88
ограничение возможностей 88
Создать команду (CRTCMD), команда 88

ALWOBIDIF (разрешить различия в объектах), параметр 264

ANSLIN (Линия - Ответ), команда
контроль объекта 562

ANSQST (Ответить на вопросы), команда
необходимые права доступа к объектам 495
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZBESTMDL
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZBESTMDL (Анализировать модель BEST/1), команда
необходимые права доступа к объектам 483

ANZCMDPFR, команда
необходимые права доступа к объектам 483

ANZDBF
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZDBF (Анализировать файл базы данных), команда
необходимые права доступа к объектам 483

ANZDBFKEY
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZDBFKEY (Анализировать ключи файла базы данных), команда
необходимые права доступа к объектам 483

ANZDFTPWD (Анализировать пароли по умолчанию), команда
необходимые права доступа к объектам 520
описание 749
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZJVM
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZJVM, команда
необходимые права доступа к объектам 437

ANZOBJCVN
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZPFRDT2 (Анализировать базу данных статистики), команда
необходимые права доступа к объектам 483

ANZPFRDTA
пользовательские профайлы, поставляемые IBM, с правами доступа 348

ANZPFRDTA (Анализировать базу данных статистики), команда
необходимые права доступа к объектам 483

ANZPGM (Анализировать программу), команда
контроль объекта 572

- ANZPGM (Анализировать программу), команда *(продолжение)*
необходимые права доступа к объектам 483
- ANZPRB (Анализировать неполадку), команда
необходимые права доступа к объектам 489
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- ANZPRFACT
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- ANZPRFACT (Анализировать операции профайлов), команда
необходимые права доступа к объектам 520
описание 749
создание исключений для пользователей 749
- ANZQRY (Анализировать запрос), команда
контроля объекта 575
необходимые права доступа к объектам 494
- ANZS34OCL (Анализировать OCL System/34), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- ANZS34OCL (Анализировать OCL System/36), команда
необходимые права доступа к объектам 469
- ANZS36OCL (Анализировать OCL System/36), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- AP (принятые права доступа), тип записи журнала 292
- AP (принятые права доступа), формат файла 611
- API (интерфейс прикладных программ) уровень защиты 40 16
- APYJRNCHGX (Применить дополнительно зарегистрированные изменения), команда
контроля объекта 551, 559
- APYPTF (Применить временное исправление программы), команда
необходимые права доступа к объектам 502
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- APYRMTPTF (Применить удаленное временное исправление программы), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- ASKQST (Задать вопрос), команда
необходимые права доступа к объектам 495
- ASTLVL (уровень поддержки), параметр пользовательский профайл 84
- ATNPGM (программа обработки клавиши Attention), параметр
пользовательский профайл 109
- Attention (ATTN), клавиша
принятые права доступа 158
- AU (изменение атрибутов), формат файла 611
- AUDLVL (уровень контроля), параметр *CMD (текст команды), значение 288
пользовательский профайл 118
- AUT (права доступа), параметр настройка списка прав доступа (*AUTL) 174
пользовательский профайл 117
создание библиотек 165
создание объектов 166
- AUTCHK (права на исправление), параметр 223
authentication
цифровой ИД 121
- AUTOCFG (автоматическая настройка устройств), значение 40
- B**
- BCHJOB (Пакетное задание), команда
необходимые права доступа к объектам 437
- BRM (QBRMS), пользовательский профайл 339
- C**
- CA (изменение прав доступа), тип записи журнала 297
- CA (изменение прав доступа), формат файла 612
- CALL (Вызвать программу), команда
необходимые права доступа к объектам 490
передача принятых прав доступа 157
- CCSID (идентификатор набора символов), параметр
пользовательский профайл 111
- CD (командная строка), формат файла 615
- CD (текст команды), тип записи журнала 288
- CFGDSTSRV (Настроить службы рассылки), команда
необходимые права доступа к объектам 395
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- CFGIPS (Настроить интерфейс IP для SNA), команда
необходимые права доступа к объектам 373
- CFGRPDS (Настроить мост VM/MVS), команда
необходимые права доступа к объектам 395
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- CFGSYSSEC (Настроить защиту системы), команда
необходимые права доступа к объектам 502
описание 335, 759
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- CFGTCP (Настроить TCP/IP), команда
объект необходимые права доступа 517
- CFGTCPAPP (Настроить приложения TCP/IP), команда
необходимые права доступа к объектам 517
- CFGTCPLPD (Настроить LPD TCP/IP), команда
необходимые права доступа к объектам 517
- CFGTCPSMTP (Настроить SMTP TCP/IP), команда
необходимые права доступа к объектам 517
- CFGTCPTELN (Настроить TELNET TCP/IP), команда
необходимые права доступа к объектам 517
описание 749
- CHGACGCDE (Изменить код учета ресурсов), команда
необходимые права доступа к объектам 437
связь с пользовательским профайлом 105
- CHGACTPRFL (Изменить список активных профайлов), команда
необходимые права доступа к объектам 520
описание 749
- CHGACTSCDE
пользовательские профайлы, поставляемые IBM, с правами доступа 348
- CHGACTSCDE (Изменить запись расписания активации), команда
необходимые права доступа к объектам 520
описание 749
- CHGAJE (Изменить запись автоматического задания), команда
контроля объекта 577
необходимые права доступа к объектам 511
- CHGALRACNE (Изменить запись о действии при получении предупреждения), команда
контроля объекта 555
необходимые права доступа к объектам 411

CHGALRD (Изменить описание предупреждения), команда контроля объекта 531
необходимые права доступа к объектам 373

CHGALRSLTE (Изменить запись о выборе предупреждений), команда контроля объекта 555
необходимые права доступа к объектам 411

CHGALRTBL (Изменить таблицу предупреждений), команда контроля объекта 531
необходимые права доступа к объектам 373

CHGASPA
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGASPA, команда 390

CHGASPACT
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGASPACT, команда
необходимые права доступа к объектам 390

CHGATR (Изменить атрибут), команда контроля объекта 540

CHGATR (Изменить атрибуты), команда контроля объекта 540

CHGAUD (Изменить параметры контроля), команда контроля объекта 541, 579, 584
необходимые права доступа к объектам 416
описание 328, 331

CHGAUT (Изменить права доступа), команда 167
контроля объекта 541, 579, 584
необходимые права доступа к объектам 416
описание 328

CHGAUTLE (Изменить запись списка прав доступа), команда
использование 175
контроля объекта 531
необходимые права доступа к объектам 375
описание 327

CHGBCKUP (Изменить опции резервного копирования), команда
необходимые права доступа к объектам 477

CHGCDDEFNT (Изменить кодированный шрифт)
права доступа к объектам, необходимые для применения команд 372

CHGCFGL (Изменить список конфигурации), команда контроля объекта 533
необходимые права доступа к объектам 385

CHGCFGLE (Изменить запись списка конфигурации), команда контроля объекта 533

CHGCFGLE (Изменить запись списка конфигурации), команда (продолжение)
необходимые права доступа к объектам 385

CHGCLNUP (Изменить список очистки), команда
необходимые права доступа к объектам 477

CHGCLS (Изменить класс), команда контроля объекта 535
необходимые права доступа к объектам 377

CHGCLUCFG
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCLUCFG, команда
необходимые права доступа к объектам 379

CHGCLUNODE
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCLUNODE, команда
необходимые права доступа к объектам 379

CHGCLURCY
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCLUVER
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCLUVER, команда
необходимые права доступа к объектам 379

CHGCM (Изменить команду), команда
ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
PRDLIB (рабочая библиотека), параметр 220
контроля объекта 535
необходимые права доступа к объектам 382
риск нарушения безопасности 220

CHGCMDCRQA (Изменить операцию запроса на изменение команды), команда контроля объекта 534
необходимые права доступа к объектам 377
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCMDDFT (Изменить параметры команды по умолчанию), команда
использование 248
контроля объекта 535
необходимые права доступа к объектам 382

CHGCMNE (Изменить запись средств связи), команда контроля объекта 577
необходимые права доступа к объектам 511

CHGCNNL (Изменить список соединений), команда
контроля объекта 536

CHGCNNLE (Изменить запись списка соединений), команда контроля объекта 536

CHGCOMSNMP (Изменить взаимодействие для SNMP), команда
объект необходимые права доступа 517

CHGCOSD (Изменить описание класса обслуживания), команда контроля объекта 537
необходимые права доступа к объектам 378

CHGCRG
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCRG, команда
необходимые права доступа к объектам 379

CHGCRGDEVE
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCRGDEVE, команда
необходимые права доступа к объектам 380

CHGCRGPRI
пользовательские профайлы, поставляемые IBM, с правами доступа 348

CHGCRGPRI, команда
необходимые права доступа к объектам 380

CHGCRQD (Изменить описание запроса на изменение), команда контроля объекта 534
необходимые права доступа к объектам 377

CHGCRSDMNK (Изменить междоменный ключ шифрования ключа), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGCSI (Изменить исходную информацию связи), команда контроля объекта 537
необходимые права доступа к объектам 383

CHGCSPPGM (Изменить программу CSP/AE), команда контроля объекта 571

CHGCTLAPPC (Изменить описание контроллера APPC), команда
необходимые права доступа к объектам 386

CHGCTLASC (Изменить описание асинхронного контроллера), команда
необходимые права доступа к объектам 386

CHGCTLBSC (Изменить описание контроллера BSC), команда
необходимые права доступа к объектам 386

CHGCTLFNC (Изменить описание финансового контроллера), команда
необходимые права доступа к объектам 386

CHGCTLHOST (Изменить описание контроллера хоста SNA), команда
необходимые права доступа к объектам 386

CHGCTLLWS (Изменить описание контроллера локальной рабочей станции), команда
необходимые права доступа к объектам 386

CHGCTLNET (Изменить описание сетевого контроллера), команда
необходимые права доступа к объектам 386

CHGCTLRRTL (Изменить описание контроллера розничной торговли), команда
необходимые права доступа к объектам 386

CHGCTLRWS (Изменить описание контроллера удаленной рабочей станции), команда
необходимые права доступа к объектам 386

CHGCTLTAP (Изменить описание контроллера лентопротяжных устройств), команда
необходимые права доступа к объектам 386

CHGCTLVWS (Изменить описание контроллера виртуальной рабочей станции), команда
необходимые права доступа к объектам 386

CHGCURDIR (Изменить текущий каталог), команда
контроля объекта 542

CHGCURLIB (Изменить текущую библиотеку), команда
необходимые права доступа к объектам 456
ограничение 221

CHGDBG (Изменить параметры отладки), команда
необходимые права доступа к объектам 490

CHGDDMF (Изменить файл Управления распределенными данными), команда
контроля объекта 551
необходимые права доступа к объектам 405

CHGDEVAPPC (Изменить описание устройства APPC), команда
необходимые права доступа к объектам 390

CHGDEVASC (Изменить описание асинхронного устройства), команда
необходимые права доступа к объектам 390

CHGDEVASP (Изменить описание устройства ASP), команда
необходимые права доступа к объектам 390

CHGDEVBSC (Изменить описание устройства BSC), команда
необходимые права доступа к объектам 390

CHGDEVCRP, команда
необходимые права доступа к объектам 390

CHGDEVDKT (Изменить описание дисководов), команда
необходимые права доступа к объектам 390

CHGDEVDSP (Изменить описание дисплея), команда
необходимые права доступа к объектам 390

CHGDEVFNC (Изменить описание финансового устройства), команда
необходимые права доступа к объектам 390

CHGDEVHOST (Изменить описание хоста SNA), команда
необходимые права доступа к объектам 390

CHGDEVINTR (Изменить описание внутрисистемного устройства), команда
необходимые права доступа к объектам 390

CHGDEVMLB, команда
необходимые права доступа к объектам 390

CHGDEVNET (Изменить описание сетевого устройства), команда
необходимые права доступа к объектам 390

CHGDEVNWSH, команда
необходимые права доступа к объектам 390

CHGDEVLOPT (Изменить описание оптического накопителя), команда
необходимые права доступа к объектам 390

CHGDEVOPT (Изменить описание устройства (оптический накопитель)), команда
необходимые права доступа к объектам 478

CHGDEVPRRT (Изменить описание принтера), команда
необходимые права доступа к объектам 390

CHGDEVRTL (Изменить описание устройства розничной торговли), команда
необходимые права доступа к объектам 390

CHGDEVSNPT (Изменить описание устройства SNTP), команда
необходимые права доступа к объектам 390

CHGDEVSNUF (Изменить описание устройства SNUF), команда
необходимые права доступа к объектам 391

CHGDEVTAP (Изменить описание лентопротяжного устройства), команда
необходимые права доступа к объектам 391

CHGDIRE (Изменить запись каталога), команда
необходимые права доступа к объектам 393
описание 333

CHGDIRSHD (Изменить теневой каталог), команда
необходимые права доступа к объектам 393

CHGDIRSRVA (Изменить атрибуты сервера каталогов), команда
необходимые права доступа к объектам 394

CHGDIRSRVA command
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGDKTF (Изменить файл дискеты), команда
контроля объекта 551
необходимые права доступа к объектам 405

CHGDLOAUD (Изменить контроль объекта библиотеки документов), команда
*AUDIT (контроль), специальные права доступа 93

CHGDLOAUD (Изменить параметры контроля объекта библиотеки документов), команда
QAUDCTL (Управление контролем), системное значение 69
контроля объекта 545
описание 331, 332

CHGDLOAUT (Изменить контроль за объектом библиотеки документов), команда
необходимые права доступа к объектам 396

CHGDLOAUT (Изменить права доступа к объекту библиотеки документов), команда
контроля объекта 545
необходимые права доступа к объектам 396
описание 332

CHGDLOOWN (Изменить владельца объекта библиотеки документов), команда
контроля объекта 545
необходимые права доступа к объектам 397
описание 332

CHGDLOPGP (Изменить основную группу объекта библиотеки документов), команда
контроля объекта 545
необходимые права доступа к объектам 397
описание 332

CHGDOCD (Изменить описание документа), команда
контроля объекта 545

CHGDOCD (Изменить описание документа), команда *(продолжение)* необходимые права доступа к объектам 397

CHGDSPF (Изменить файл дисплея), команда
контроля объекта 551
необходимые права доступа к объектам 405

CHGDSTD (Изменить описание рассылки), команда
контроля объекта 545
необходимые права доступа к объектам 395

CHGDSTL (Изменить список рассылки), команда
необходимые права доступа к объектам 396

CHGDSTPWD (Изменить пароль Специальных сервисных средств), команда
необходимые права доступа к объектам 520
описание 329

CHGDSTQ (Изменить очередь рассылки), команда
необходимые права доступа к объектам 395
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGDSTRTE (Изменить маршрут рассылки), команда
необходимые права доступа к объектам 395
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGDTA (Изменить данные), команда
необходимые права доступа к объектам 405

CHGDTAARA (Изменить область данных), команда
контроля объекта 547
необходимые права доступа к объектам 389

CHGEMLCFGE (Изменить запись конфигурации эмуляции), команда
необходимые права доступа к объектам 392

CHGENVVAR (Изменить переменную среды), команда
необходимые права доступа к объектам 403

CHGEWCBCDE (Изменить запись штрихового кода для контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 403

CHGEWCM (Изменить элемент контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 403

CHGEWCPTCE (Изменить запись PTC контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 404

CHGEWLM (Изменить элемент линии расширенной беспроводной сети), команда
необходимые права доступа к объектам 404

CHGEXPCDE (Изменить запись расписания истечения срока), команда
необходимые права доступа к объектам 520
описание 749
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGFCNARA (пользовательские профайлы, поставляемые IBM, с правами доступа 349)

CHGFCT (Изменить таблицу управления формами), команда
необходимые права доступа к объектам 498

CHGFCTE (Изменить запись таблицы управления формами), команда
необходимые права доступа к объектам 498

CHGFNTTBLE (Изменить запись таблицы шрифтов DBCS)
права доступа к объектам, необходимые для применения команд 372

CHGFTR (Изменить фильтр), команда
контроля объекта 555
необходимые права доступа к объектам 411

CHGGPHFMT (пользовательские профайлы, поставляемые IBM, с правами доступа 349)

CHGGPHFMT (Изменить графический формат), команда
необходимые права доступа к объектам 483

CHGGPHPKG (Изменить графический пакет), команда
необходимые права доступа к объектам 483
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGGRPA (Изменить атрибуты группы), команда
необходимые права доступа к объектам 438

CHGHLLPTR (Изменить указатель языка высокого уровня), команда
необходимые права доступа к объектам 490

CHGICFDEVE (Изменить запись об устройстве функции межсистемной связи), команда
необходимые права доступа к объектам 405

CHGICFF (Изменить файл функции межсистемной связи), команда
необходимые права доступа к объектам 405

CHGIMGCLG, команда
необходимые права доступа к объектам 414

CHGIMGCLGE, команда
необходимые права доступа к объектам 414

CHGIPLA, команда 437

CHGIPSIFC (Изменить интерфейс IP для SNA), команда
необходимые права доступа к объектам 373

CHGIPSLOC (Изменить запись о расположении IP для SNA), команда
необходимые права доступа к объектам 373

CHGIPSTOS (Изменить тип обслуживания IP для SNA), команда
необходимые права доступа к объектам 373

CHGJOB (Изменить задание), команда
контроля объекта 558
необходимые права доступа к объектам 438
принятые права доступа 158

CHGJOB (Изменить описание задания), команда
контроля объекта 557
необходимые права доступа к объектам 441

CHGJOBQ (Изменить очередь заданий), команда
контроля объекта 557
необходимые права доступа к объектам 442

CHGJOBQE (Изменить запись очереди заданий), команда
контроля объекта 558, 577
необходимые права доступа к объектам 511

CHGJOBSCDE (Изменить запись расписания заданий), команда
контроля объекта 558
необходимые права доступа к объектам 443

CHGJOBTRC (пользовательские профайлы, поставляемые IBM, с правами доступа 349)

CHGJOBTYP (Изменить тип задания), команда
необходимые права доступа к объектам 483
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGJRN (Заменить журнал), команда
контроля объекта 559, 560
необходимые права доступа к объектам 444
отключение получателя 311, 312
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGJRNOBJ (Изменить объект с журналом), команда
контроля объекта 528

CHGLANADPI (Изменить информацию об адаптере LAN), команда
необходимые права доступа к объектам 464

CHGLF (Изменить логический файл), команда
контроля объекта 552
необходимые права доступа к объектам 405

CHGLFM (Изменить элемент логического файла), команда
контроля объекта 552
необходимые права доступа к объектам 405

CHGLIB (Изменить библиотеку), команда
контроля объекта 561
необходимые права доступа к объектам 456

CHGLIBL (Изменить список библиотек), команда
использование 218
необходимые права доступа к объектам 456

CHGLIBOWN (Изменить владельца библиотеки), инструмент 255

CHGLICINF (Изменить информацию о лицензии), команда
необходимые права доступа к объектам 461
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGLINASC (Изменить описание линии асинхронной связи), команда
необходимые права доступа к объектам 462

CHGLINBSC (Изменить описание линии двоичной синхронной связи), команда
необходимые права доступа к объектам 462

CHGLINETH (Изменить описание линии (Ethernet)), команда
необходимые права доступа к объектам 462

CHGLINFAX (Изменить описание линии факсимильной связи), команда
необходимые права доступа к объектам 462

CHGLINFR (Изменить описание линии (сеть Frame Relay)), команда
необходимые права доступа к объектам 462

CHGLINIDD (Изменить описание линии (сеть DDI)), команда
необходимые права доступа к объектам 462

CHGLINS DLC (Изменить описание линии (SDLC)), команда
необходимые права доступа к объектам 462

CHGLINTDLC (Изменить описание линии (TDLC)), команда
необходимые права доступа к объектам 462

CHGLINTRN (Изменить описание линии (сеть Token-Ring)), команда
необходимые права доступа к объектам 462

CHGLINWLS (Изменить описание беспроводной линии), команда
необходимые права доступа к объектам 462

CHGLINX25 (Изменить описание линии (X.25)), команда
необходимые права доступа к объектам 462

CHGLPDA (Изменить атрибуты LPD), команда
необходимые права доступа к объектам 517

CHGMGDSYSA (Изменить атрибуты управляемой системы), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGMGRSRVA (Изменить атрибуты службы диспетчера), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGMGTCOL, команда
необходимые права доступа к объектам 483

CHGMENU (Изменить меню), команда
PRDLIB (рабочая библиотека), параметр 220
контроля объекта 563
необходимые права доступа к объектам 465
риск нарушения безопасности 220

CHGMOD (Изменить модуль), команда
контроля объекта 564
необходимые права доступа к объектам 470

CHGMODD (Изменить описание режима), команда
контроля объекта 564
необходимые права доступа к объектам 469

CHGMSGD (Изменить описание сообщения), команда
контроля объекта 565
необходимые права доступа к объектам 467

CHGMSGF (Изменить файл сообщений), команда
контроля объекта 565
необходимые права доступа к объектам 468

CHGMSGQ (Изменить очередь сообщений), команда
контроля объекта 566
необходимые права доступа к объектам 468

CHGMSTK (Изменить главный ключ), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGMWSD (Изменить описание сетевого сервера), команда
контроля объекта 568

CHGNETA (Изменить сетевые атрибуты), команда
использование 225
необходимые права доступа к объектам 471
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGNETJOBE (Изменить запись сетевого задания), команда
необходимые права доступа к объектам 471
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGNFSEXP (Изменить запись экспорта NFS), команда
необходимые права доступа к объектам 472
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGNTBD (Изменить описание NetBIOS), команда
контроля объекта 567
необходимые права доступа к объектам 470

CHGNWIFR (Изменить описание сетевого интерфейса (Frame Relay)), команда
необходимые права доступа к объектам 473

CHGNWIISDN (Изменить описание сетевого интерфейса для ISDN), команда
контроля объекта 567

CHGNWSA (Изменить атрибут сетевого сервера), команда
необходимые права доступа к объектам 474

CHGNWSA (Изменить атрибуты сетевого сервера), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGNWSALS (Изменить псевдоним сетевого сервера), команда
необходимые права доступа к объектам 474

CHGNWSCFG, команда
необходимые права доступа к объектам 475
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGNWSD (Изменить описание сетевого сервера), команда
необходимые права доступа к объектам 475

CHGNWSSTG (Изменить область памяти сетевого сервера), команда
необходимые права доступа к объектам 473

CHGNWSVRA (Создать атрибут сетевого сервера), команда
необходимые права доступа к объектам 473

CHGOBJAUD (Изменить контроль объекта), команда
*AUDIT (контроль), специальные права доступа 93
QAUDCTL (Управление контролем), системное значение 69
описание 328

CHGOBJAUD (Изменить параметры контроля объекта), команда
необходимые права доступа к объектам 364
описание 331

CHGOBJCRQA (Изменить операцию запроса на изменение объекта), команда
контроля объекта 534
необходимые права доступа к объектам 377
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGOBJD (Изменить описание объекта), команда
контроля объекта 528
необходимые права доступа к объектам 364

CHGOBJOWN (Изменить владельца объекта), команда
использование 171
контроля объекта 528
необходимые права доступа к объектам 364
описание 328

CHGOBJPGP (Изменить основную группу объекта), команда 152, 172
необходимые права доступа к объектам 364
описание 328

CHGORTA (Изменить оптические атрибуты), команда
необходимые права доступа к объектам 478
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGORTVOL (Изменить оптический том), команда
необходимые права доступа к объектам 478

CHGOUTQ (Изменить очередь вывода), команда
использование 222
контроля объекта 569
необходимые права доступа к объектам 481

CHGOWN (Изменить владельца), команда 171
контроля объекта 541, 579, 584, 587
необходимые права доступа к объектам 417
описание 328

CHGPCST (Изменить ограничение для физического файла), команда
необходимые права доступа к объектам 405

CHGPDGPRF (Изменить профайл группы дескрипторов печати), команда
контроля объекта 571
необходимые права доступа к объектам 489

CHGPEXDFN (Изменить определение PEX), команда
необходимые права доступа к объектам 483
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGPF (Изменить физический файл), команда
контроля объекта 552
необходимые права доступа к объектам 405

CHGPFCNARA (Изменить функциональную область), команда
необходимые права доступа к объектам 483

CHGPFCST (Изменить ограничение для физического файла), команда
контроля объекта 552

CHGPFM (Изменить элемент физического файла), команда
контроля объекта 552
необходимые права доступа к объектам 405

CHGPFTRG (Изменить триггер для физического файла), команда
контроля объекта 553
необходимые права доступа к объектам 405

CHGPGM (Изменить программу), команда
контроля объекта 571
настройка параметра USEADPAUT 160
необходимые права доступа к объектам 490

CHGPGMVAR (Изменить переменную программы), команда
необходимые права доступа к объектам 490

CHGPGP (Изменить основную группу), команда 172
контроля объекта 541, 579, 584, 587
необходимые права доступа к объектам 417
описание 328

CHGPJ (Изменить предварительное задание), команда
необходимые права доступа к объектам 438

CHGRJE (Изменить запись предварительного задания), команда
контроля объекта 577
необходимые права доступа к объектам 511

CHGPRB (Изменить неполадку), команда
необходимые права доступа к объектам 489

CHGPRB (Изменить неполадку), команда
(продолжение)
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGPRBACNE (Изменить запись о действии в случае неполадки), команда
контроля объекта 555
необходимые права доступа к объектам 411, 489

CHGPRBSLTE (Изменить запись о выборе неполадок), команда
контроля объекта 555
необходимые права доступа к объектам 411, 489

CHGPRDCRQA (Изменить операцию запроса на изменение продукта), команда
контроля объекта 534
необходимые права доступа к объектам 377
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGPRF (Изменить профайл), команда
использование 127
контроля объекта 589
необходимые права доступа к объектам 520
описание 330

CHGPRTF (Изменить файл принтера), команда
контроля объекта 552
необходимые права доступа к объектам 405

CHGPSFCFG (Изменить конфигурацию Print Services Facility), команда
необходимые права доступа к объектам 489

CHGPTFCRQA (Изменить операцию запроса на изменение PTF), команда
контроля объекта 534
необходимые права доступа к объектам 377
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGPTR (Изменить указатель), команда
необходимые права доступа к объектам 490
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGPWD (Изменить пароль), команда
контроля объекта 589
необходимые права доступа к объектам 520
описание 329
параметров контроля 273
применение пароля, системные значения 50
указание пароля, совпадающего с именем пользователя 81

CHGPWRSCD (Изменить расписание включения и выключения питания), команда
необходимые права доступа к объектам 477

CHGPWRSCDE (Изменить запись расписания включения и выключения питания), команда
необходимые права доступа к объектам 477

CHGQRYA (Изменить атрибут запроса), команда
необходимые права доступа к объектам 494

CHGQSTDB (Изменить базу данных вопросов и ответов), команда
необходимые права доступа к объектам 495
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGRCYAP (Изменить восстановление путей доступа), команда
контроля объекта 530
необходимые права доступа к объектам 372
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGRDBDIRE (Изменить запись каталога реляционной базы данных), команда
необходимые права доступа к объектам 497

CHGRJECMNE (Изменить запись средств связи RJE), команда
необходимые права доступа к объектам 498

CHGRJERDRE (Изменить запись программы чтения RJE), команда
необходимые права доступа к объектам 498

CHGRJEWTRE (Изменить запись программы записи RJE), команда
необходимые права доступа к объектам 499

CHGRMTJRN (Изменить удаленный журнал), команда
контроля объекта 559

CHGRPYLE (Изменить запись списка ответов), команда
контроля объекта 576
необходимые права доступа к объектам 513
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGRSCCRQA (Изменить операцию запроса на изменение ресурса), команда
контроля объекта 535
необходимые права доступа к объектам 377
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGRTGE (Изменить запись о выполнении), команда
контроля объекта 577

CHGRTGE (Изменить запись о выполнении), команда (*продолжение*)
необходимые права доступа к объектам 511

CHGS34LIBM (Изменить элементы библиотек System/34), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGS36 (Изменить System/36), команда
контроля объекта 587
необходимые права доступа к объектам 513

CHGS36A (Изменить атрибуты System/36), команда
контроля объекта 587
необходимые права доступа к объектам 513

CHGS36PGMA (Изменить атрибуты программы System/36), команда
контроля объекта 572
необходимые права доступа к объектам 513

CHGS36PRCA (Изменить атрибуты процедуры System/36), команда
контроля объекта 552
необходимые права доступа к объектам 513

CHGS36SRCA (Изменить атрибуты исходного текста System/36), команда
необходимые права доступа к объектам 513

CHGSAVF (Изменить файл сохранения), команда
контроля объекта 552
необходимые права доступа к объектам 405

CHGSBSD (Изменить описание подсистемы), команда
контроля объекта 577
необходимые права доступа к объектам 511

CHGSCHIDX (Изменить индекс поиска), команда
контроля объекта 578
необходимые права доступа к объектам 436

CHGSECA (Изменить атрибуты защиты), команда
необходимые права доступа к объектам 502

CHGSECAUD (Изменить контроль действий)
функция контроля за действиями 308

CHGSECAUD (Изменить контроль действий), команда
описание 334, 751

CHGSECAUD (Изменить параметры контроля за действиями), команда
необходимые права доступа к объектам 502

CHGSHRPOOL (Изменить общий пул памяти), команда
необходимые права доступа к объектам 512

CHGSNMPA (Изменить атрибуты SNMP), команда
необходимые права доступа к объектам 517

CHGSPLFA (Изменить атрибуты буферного файла), команда
DSPDTA, параметр очереди вывода 222
действие, контроль 581
контроля объекта 569
необходимые права доступа к объектам 508

CHGSRCPF (Изменить исходный физический файл), команда
необходимые права доступа к объектам 405

CHGSRVA (Изменить служебные атрибуты), команда
необходимые права доступа к объектам 503

CHGSRVPGM (Изменить служебную программу), команда
контроля объекта 583
настройка параметра USEADPAUT 160
необходимые права доступа к объектам 491

CHGSSND (Изменить описание сеанса), команда
необходимые права доступа к объектам 499

CHGSSNMAX (Изменить максимальное число сеансов), команда
контроля объекта 564
необходимые права доступа к объектам 469

CHGSVRAUTE (Изменить запись идентификации сервера), команда
необходимые права доступа к объектам 502

CHGSYSDIRA (Изменить атрибуты системного каталога), команда
контроля объекта 543
необходимые права доступа к объектам 393

CHGSYSJOB (Изменить системное задание), команда
необходимые права доступа к объектам 438

CHGSYSLIBL (Изменить список системных библиотек), команда
использование 218
необходимые права доступа к объектам 456
пользовательские профайлы, поставляемые IBM, с правами доступа 349
пример программы 239

CHGSYSVAL (Изменить системное значение), команда
необходимые права доступа к объектам 513
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHGTAPCTG (Заменить кассету магнитной ленты), команда
необходимые права доступа к объектам 464

CHGTAPF (Изменить файл магнитной ленты), команда
контроля объекта 552
необходимые права доступа к объектам 405

CHGTCPRA (Изменить атрибуты TCP/IP), команда
необходимые права доступа к объектам 517

CHGTCPHTE (Изменить запись таблицы хостов TCP/IP), команда
необходимые права доступа к объектам 517

CHGTCPHFC (Изменить интерфейс TCP/IP), команда
необходимые права доступа к объектам 517

CHGTCPRTE (Изменить запись маршрута TCP/IP), команда
необходимые права доступа к объектам 517

CHGTELNA (Изменить атрибуты TELNET), команда
необходимые права доступа к объектам 517

CHGTIMZON, команда 518

CHGUSRAUD (Изменить контроль пользователей), команда
*AUDIT (контроль), специальные права доступа 93
QAUDCTL (Управление контролем), системное значение 69
использование 132
необходимые права доступа к объектам 520
описание 330, 331

CHGUSRAUD (Изменить контроль), команда
использование 132

CHGUSRPRF (Изменить пользовательский профайл), команда
использование 127
контроля объекта 589
необходимые права доступа к объектам 520
описание 329, 330
состав пароля, системные значения 50
указание пароля, совпадающего с именем пользователя 81

CHGUSRTRC (Изменить пользовательскую трассировку), команда
необходимые права доступа к объектам 438

CHGVTMAR (Изменить раскладку клавиатуры VT), команда
необходимые права доступа к объектам 517

CHGWSE (Изменить запись рабочей станции), команда
контроля объекта 577
необходимые права доступа к объектам 511

CHGWTR (Изменить загрузчик), команда
необходимые права доступа к объектам 524

CHKASPBAL
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHKCMNTRC (Проверить трассировку соединений), команда
необходимые права доступа к объектам 503
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHKDKT (Проверить дискету), команда
необходимые права доступа к объектам 464

CHKDLO (Проверить объект библиотеки документов), команда
необходимые права доступа к объектам 397

CHKDNSCFG (Утилита настройки DNS), команда
необходимые права доступа к объектам 401

CHKDNSZNE (Утилита зон DNS), команда
необходимые права доступа к объектам 401

CHKDOC (Проверить документ), команда
контроля объекта 544
необходимые права доступа к объектам 397

CHKIGCTBL (Проверить таблицу шрифтов DBCS), команда
контроля объекта 557

CHKIN (Вернуть), команда
контроля объекта 579, 584
необходимые права доступа к объектам 418

CHKMSTKVV, команда
необходимые права доступа к объектам 388

CHKOBJ (Проверить объект), команда
контроля объекта 529
необходимые права доступа к объектам 364

CHKOBJTG (Проверить целостность объекта), команда 3
контроль использования 277
необходимые права доступа к объектам 365
описание 322, 330, 754

CHKOUT (Изъять), команда
контроля объекта 579, 584
необходимые права доступа к объектам 418

CHKPRDOPT (Проверить компонент продукта), команда
необходимые права доступа к объектам 503
пользовательские профайлы, поставляемые IBM, с правами доступа 349

CHKPWD (Проверить пароль), команда
использование 133
контроля объекта 589

CHKPWD (Проверить пароль), команда
(продолжение)
необходимые права доступа к объектам 520
описание 329

CHKTAP (Проверить магнитную ленту), команда
необходимые права доступа к объектам 464

CHRIDCTL (опции пользователя), параметр
пользовательский профайл 112

CLP38, программы 144

CLRDKT (Очистить дискету), команда
необходимые права доступа к объектам 465

CLRJOBQ (Очистить очередь заданий), команда
контроля объекта 557
необходимые права доступа к объектам 442

CLRLIB (Очистить библиотеку), команда
контроля объекта 561
необходимые права доступа к объектам 457

CLRMSGQ (Очистить очередь сообщений), команда
контроля объекта 566
необходимые права доступа к объектам 468

CLRMSTKEY, команда
необходимые права доступа к объектам 388

CLROUTQ (Очистить очередь вывода), команда
действие, контроль 582
контроля объекта 569
необходимые права доступа к объектам 481

CLRPFM (Очистить элемент физического файла), команда
контроля объекта 552
необходимые права доступа к объектам 405

CLRSVAVF (Очистить файл сохранения), команда
необходимые права доступа к объектам 405

CLRTRCDTA (Очистить данные трассировки), команда
необходимые права доступа к объектам 491

CMPJRNIMG (Сравнить образы журнала), команда
контроля объекта 559
необходимые права доступа к объектам 444

CNLRJERDR (Отменить чтение RJE), команда
необходимые права доступа к объектам 499

CNLRJEWTR (Отменить запись RJE), команда
необходимые права доступа к объектам 499

CNTRYID (идентификатор страны или региона), параметр
пользовательский профайл 111

CO (создание объекта), формат файла 616

CO (создать объект), тип записи журнала 151, 288

COMMIT (Фиксировать), команда
необходимые права доступа к объектам 383

CP (изменение пользовательского профайла), тип записи журнала 294

CP (изменение пользовательского профайла), формат файла 618

CPHDTA (Зашифровать данные), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CPROBJ (Сжать объект), команда
контроля объекта 529
необходимые права доступа к объектам 365

CPY (Скопировать объект), команда
контроля объекта 540

CPY (Скопировать), команда
контроля объекта 541, 584, 585, 586, 587
необходимые права доступа к объектам 419

CPYAUDJRNE, команда
необходимые права доступа к объектам 444

CPYCFGL (Скопировать список конфигурации), команда
контроля объекта 533
необходимые права доступа к объектам 385

CPYCNARA (Скопировать функциональную область), команда
необходимые права доступа к объектам 484

CPYDOC (Скопировать документ), команда
контроля объекта 544, 545
необходимые права доступа к объектам 397

CPYF (Скопировать файл), команда
контроля объекта 550, 552
необходимые права доступа к объектам 405

CPYFRMDIR (Скопировать из каталога), команда
необходимые права доступа к объектам 393

CPYFRMDKT (Скопировать с дискеты), команда
необходимые права доступа к объектам 406

CPYFRMIMPF (Скопировать из файла импорта), команда
необходимые права доступа к объектам 406

CPYFRMLDIF (Скопировать из LDIF), команда
необходимые права доступа к объектам 394

CPYFRMQRYF (Скопировать из файла запроса), команда
необходимые права доступа к объектам 406

CPYFRMSTMF (Скопировать из потокового файла), команда
необходимые права доступа к объектам 406

CPYFRMTAP (Скопировать с магнитной ленты), команда
необходимые права доступа к объектам 406

CPYGRPHFMT
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CPYGRPHFMT (Скопировать графический формат), команда
необходимые права доступа к объектам 484

CPYGRHPKG
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CPYGRHPKG (Скопировать графический пакет), команда
необходимые права доступа к объектам 484

CPYIGCSRT (Скопировать таблицу сортировки DBCS), команда
контроля объекта 556

CPYIGCTBL (Скопировать таблицу шрифтов DBCS), команда
контроля объекта 556
необходимые права доступа к объектам 402

CPYLIV (Скопировать библиотеку), команда
необходимые права доступа к объектам 457

CPYOPT (Скопировать оптический носитель), команда
необходимые права доступа к объектам 478

CPYPRFCOL (Скопировать базу данных статистики), команда
необходимые права доступа к объектам 484
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CPYPRFRDTA
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CPYPRFRDTA (Скопировать базу данных статистики), команда
необходимые права доступа к объектам 484

CPYPTF (Скопировать временное исправление программы), команда
необходимые права доступа к объектам 503

CPYPTF (Скопировать временное исправление программы), команда
(продолжение)
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CPYPTFGRP (Скопировать группу PTF), команда
необходимые права доступа к объектам 503

CPYPTFGRP (Скопировать группу временных исправлений программ), команда 350

CPYSPLF (Скопировать буферный файл), команда
DSPDTA, параметр очереди вывода 222
действие, контроль 581
контроля объекта 569
необходимые права доступа к объектам 508

CPYSRCF (Скопировать исходный файл), команда
необходимые права доступа к объектам 406

CPYTCRHT, команда
необходимые права доступа к объектам 516

CPYTODIR (Скопировать в каталог), команда
необходимые права доступа к объектам 393

CPYTODKT (Скопировать на дискету), команда
необходимые права доступа к объектам 406

CPYTOIMPF (Скопировать в файл импорта), команда
необходимые права доступа к объектам 406

CPYTOLDIF (Скопировать в LDIF), команда
необходимые права доступа к объектам 394

CPYTOSTMF (Скопировать в потоковый файл), команда
необходимые права доступа к объектам 407

CPYTOTAP (Скопировать на магнитную ленту), команда
необходимые права доступа к объектам 407

CQ (изменение *CRQD), формат файла 622

CQ (изменение объекта *CRQD), тип записи журнала 294

CRTADMDMN, команда
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CRTALRTBL (Создать таблицу предупреждений), команда
необходимые права доступа к объектам 373

CRTAUT (права при создании), параметр описание 146
просмотр 165

CRTAUT (права при создании), параметр
(продолжение)
риски 146

CRTAUTHLR (Создать владельца прав
доступа), команда
необходимые права доступа к
объектам 375
описание 327, 332
пользовательские профайлы,
поставляемые IBM, с правами
доступа 350
рекомендации 160

CRTAUTL (Создать список прав доступа),
команда
использование 174
необходимые права доступа к
объектам 375
описание 327

CRTBESTMDL (Создать модель BEST/1),
команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 350

CRTBESTMDL (Создать модель
Best/1-400), команда
необходимые права доступа к
объектам 484

CRTBNDC (Создать связанную программу
на C), команда
необходимые права доступа к
объектам 450

CRTBNDCBL (Создать связанную
программу на COBOL), команда
необходимые права доступа к
объектам 450

CRTBNDCL
необходимые права доступа к
объектам 450

CRTBNDCPP (Создать связанную
программу на CPP), команда
необходимые права доступа к
объектам 451

CRTBNDDIR (Создать каталог
связывания), команда
необходимые права доступа к
объектам 376

CRTBNDRPG (Создать связанную
программу на RPG), команда
необходимые права доступа к
объектам 451

CRTBSCF (Создать бисинхронный файл),
команда
контроля объекта 550

CRTCBLMOD (Создать модуль на
COBOL), команда
необходимые права доступа к
объектам 451

CRTCBLPGM (Создать программу на
COBOL), команда
необходимые права доступа к
объектам 452

CRTCFGL (Создать список конфигурации),
команда
необходимые права доступа к
объектам 385

CRTCKMKSF, команда
необходимые права доступа к
объектам 388

CRTCLD (Создать описание локали C),
команда
необходимые права доступа к
объектам 451

CRTCLMOD
необходимые права доступа к
объектам 451

CRTCLPGM (Создать программу на языке
CL), команда
необходимые права доступа к
объектам 452

CRTCLS (Создать класс), команда
необходимые права доступа к
объектам 378
пользовательские профайлы,
поставляемые IBM, с правами
доступа 350

CRTCLU
пользовательские профайлы,
поставляемые IBM, с правами
доступа 350

CRTCLU, команда
необходимые права доступа к
объектам 380

CRTCMD (Создать команду), команда
ALWLMTUSR (разрешить для
пользователя с ограниченными
возможностями), параметр 88
PRDLIB (рабочая библиотека),
параметр 220
необходимые права доступа к
объектам 382
риск нарушения безопасности 220

CRTCMNF (Создать файл средств связи),
команда
контроля объекта 550

CRTCMOD (Создать модуль на C),
команда
необходимые права доступа к
объектам 452

CRTCOSD (Создать описание класса
обслуживания), команда
необходимые права доступа к
объектам 378

CRTCPPMOD (Создать связанный модуль
CPP), команда
необходимые права доступа к
объектам 452

CRTCRG
пользовательские профайлы,
поставляемые IBM, с правами
доступа 350

CRTCRQD (Создать описание запроса на
изменение), команда
необходимые права доступа к
объектам 377

CRTCSI (Создать исходную информацию
связи), команда
необходимые права доступа к
объектам 384

CRTCTLAPPC (Создать описание
контроллера APPC), команда
необходимые права доступа к
объектам 386

CRTCTLASC (Создать описание
асинхронного контроллера), команда
необходимые права доступа к
объектам 386

CRTCTLBSC (Создать описание
контроллера BSC), команда
необходимые права доступа к
объектам 387

CRTCTLFNC (Создать описание
финансового контроллера), команда
необходимые права доступа к
объектам 387

CRTCTLHOST (Создать описание
контроллера хоста SNA), команда
необходимые права доступа к
объектам 387

CRTCTLLWS (Создать описание
контроллера локальной рабочей
станции), команда
необходимые права доступа к
объектам 387

CRTCTLNET (Создать описание сетевого
контроллера), команда
необходимые права доступа к
объектам 387

CRTCTLRTL (Создать описание
контроллера розничной торговли),
команда
необходимые права доступа к
объектам 387

CRTCTLRWS (Создать описание
контроллера удаленной рабочей
станции), команда
необходимые права доступа к
объектам 387

CRTCTLTAP (Создать описание
контроллера лентопротяжных
устройств), команда
необходимые права доступа к
объектам 387

CRTCTLVWS (Создать описание
контроллера виртуальной рабочей
станции), команда
необходимые права доступа к
объектам 387

CRTDDMF (Создать файл Управления
распределенными данными), команда
необходимые права доступа к
объектам 407

CRTDEVAPPC (Создать описание
устройства APPC), команда
необходимые права доступа к
объектам 391

CRTDEVASC (Создать описание
асинхронного устройства), команда
необходимые права доступа к
объектам 391

CRTDEVASP (Создать описание
устройства ASP), команда
необходимые права доступа к
объектам 391

CRTDEVBSC (Создать описание
устройства BSC), команда
необходимые права доступа к
объектам 391

CRTDEVDKT (Создать описание дисковода), команда
необходимые права доступа к объектам 391

CRTDEVDSP (Создать описание дисплея), команда
необходимые права доступа к объектам 391

CRTDEVFNC (Создать описание финансового устройства), команда
необходимые права доступа к объектам 391

CRTDEVHOST (Создать описание хоста SNA), команда
необходимые права доступа к объектам 391

CRTDEVINTR (Создать описание внутрисистемного устройства), команда
необходимые права доступа к объектам 391

CRTDEVMLB, команда
необходимые права доступа к объектам 391

CRTDEVNET (Создать описание сетевого устройства), команда
необходимые права доступа к объектам 391

CRTDEVNWSH, команда
необходимые права доступа к объектам 391

CRTDEVOPT (Создать описание оптического накопителя), команда
необходимые права доступа к объектам 391

CRTDEVOPT (Создать описание устройства (оптический накопитель)), команда
необходимые права доступа к объектам 479

CRTDEVPRNT (Создать описание принтера), команда
необходимые права доступа к объектам 391

CRTDEVRTL (Создать описание устройства ровничной торговли), команда
необходимые права доступа к объектам 391

CRTDEVSNPT (Создать описание устройства SNTP), команда
необходимые права доступа к объектам 391

CRTDEVSNUF (Создать описание устройства SNUF), команда
необходимые права доступа к объектам 391

CRTDEVTAP (Создать описание лентопротяжного устройства), команда
необходимые права доступа к объектам 391

CRTDIR (Создать каталог), команда
контроль объекта 541

CRTDKTF (Создать файл дискеты), команда
необходимые права доступа к объектам 407

CRTDOC (Создать документ), команда
необходимые права доступа к объектам 397

CRTDSPF (Создать файл дисплея), команда
контроль объекта 550
необходимые права доступа к объектам 407

CRTDSTL (Создать список рассылки), команда
необходимые права доступа к объектам 396

CRTDTAARA (Создать область данных), команда
необходимые права доступа к объектам 389

CRTDTADCT (Создать словарь данных), команда
необходимые права доступа к объектам 435

CRTDTAQ (Создать очередь данных), команда
необходимые права доступа к объектам 390

CRTDUPOBJ (Создать копию объекта), команда
контроль объекта 527
необходимые права доступа к объектам 365

CRTEDTD (Создать описание формата), команда
необходимые права доступа к объектам 403

CRTFCNARA
пользовательские профайлы, предоставляемые IBM, с правами доступа 350

CRTFCNARA (Создать функциональную область), команда
необходимые права доступа к объектам 484

CRTFCT (Создать таблицу управления формами), команда
необходимые права доступа к объектам 499

CRTFLR (Создать папку), команда
контроль объекта 545
необходимые права доступа к объектам 397

CRTFNTRSC (Создать ресурсы шрифтов), команда
необходимые права доступа к объектам 372

CRTFNNTBL (Создать таблицу шрифтов DBCS)
права доступа к объектам, необходимые для применения команд 372

CRTFORMDF (Создать определение формы), команда
необходимые права доступа к объектам 372

CRTFTR (Создать фильтр), команда
необходимые права доступа к объектам 411

CRTGDF (Создать файл графических данных), команда
контроль объекта 533

CRTGPHFMT
пользовательские профайлы, предоставляемые IBM, с правами доступа 350

CRTGPHPKG
пользовательские профайлы, предоставляемые IBM, с правами доступа 350

CRTGPHPKG (Создать графический пакет), команда
необходимые права доступа к объектам 485

CRTGSS (Создать набор графических символов), команда
необходимые права доступа к объектам 413

CRTHSTDTA
пользовательские профайлы, предоставляемые IBM, с правами доступа 350

CRTHSTDTA (Создать данные хронологии), команда
необходимые права доступа к объектам 485

CRTICFF (Создать файл ICF), команда
контроль объекта 550

CRTICFF (Создать файл функции межсистемной связи), команда
необходимые права доступа к объектам 407

CRTIGCDCT (Создать словарь преобразования DBCS), команда
необходимые права доступа к объектам 402

CRTIMGCLG, команда
необходимые права доступа к объектам 414

CRTJOB (Создать описание задания), команда
необходимые права доступа к объектам 441
пользовательские профайлы, предоставляемые IBM, с правами доступа 350

CRTJOBQ (Создать очередь заданий), команда
необходимые права доступа к объектам 442

CRTJRN (Создать журнал), команда
журнал контроля (QAUDJRN), создание 309
необходимые права доступа к объектам 444

CRTJRNRCV (Создать получатель журнала), команда
необходимые права доступа к объектам 447
создание получателя журнала контроля (QAUDJRN) 309

CRTLASREP (Создать локальный абстрактный синтаксис), команда
пользовательские профайлы, предоставляемые IBM, с правами доступа 350

CRTRJEBSFC (Создать файл BSC RJE), команда
необходимые права доступа к объектам 499

CRTRJECFG (Создать конфигурацию RJE), команда
необходимые права доступа к объектам 500

CRTRJECMNF (Создать файл связи RJE), команда
необходимые права доступа к объектам 500

CRTRNDCCFG (Утилита настройки RNDC), команда
необходимые права доступа к объектам 401

CRTRPGMOD (Создать модуль на RPG), команда
необходимые права доступа к объектам 452

CRTRPGPGM (Создать программу на RPG/400), команда
необходимые права доступа к объектам 453

CRTRPTPGM (Создать программу автоматического создания отчетов), команда
необходимые права доступа к объектам 453

CRTS36CBL (Создать System/36 COBOL), команда
необходимые права доступа к объектам 453

CRTS36DSPF (Создать файл дисплея System/36), команда
необходимые права доступа к объектам 408, 514

CRTS36MNU (Создать меню System/36), команда
необходимые права доступа к объектам 466, 514

CRTS36MSGF (Создать файл сообщений System/36), команда
необходимые права доступа к объектам 514

CRTS36RPG (Создать System/36 RPG), команда
необходимые права доступа к объектам 453

CRTS36RPGR (Создать System/36 RPGR), команда
необходимые права доступа к объектам 453

CRTS36RPT (Создать автоматический отчет System/36), команда
необходимые права доступа к объектам 453

CRTSAVF (Создать файл сохранения), команда
необходимые права доступа к объектам 408

CRTSBSD (Создать описание подсистемы), команда
необходимые права доступа к объектам 511

CRTSBSD (Создать описание подсистемы), команда *(продолжение)*
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CRTSCHIDX (Создать индекс поиска), команда
необходимые права доступа к объектам 436

CRTSPADCT (Создать орфографический словарь), команда
контроль объекта 581
необходимые права доступа к объектам 507

CRTSQLCBL (Создать SQL COBOL), команда
необходимые права доступа к объектам 454

CRTSQLCBLI (Создать объект SQL ILE COBOL), команда
необходимые права доступа к объектам 454

CRTSQLCI (Создать объект SQL ILE C), команда
необходимые права доступа к объектам 453

CRTSQLCPPI (Создать объект SQL ILE C++), команда
необходимые права доступа к объектам 454

CRTSQLFTN (Создать SQL FORTRAN), команда
необходимые права доступа к объектам 454

CRTSQLPKG (Создать пакет языка структурных запросов), команда
необходимые права доступа к объектам 482

CRTSQLPLI (Создать SQL PL/I), команда
необходимые права доступа к объектам 455

CRTSQLRPG (Создать SQL RPG), команда
необходимые права доступа к объектам 455

CRTSQLRPGI (Создать объект SQL ILE RPG), команда
необходимые права доступа к объектам 455

CRTSRCPF (Создать исходный физический файл), команда
необходимые права доступа к объектам 408

CRTSRVPGM (Создать служебную программу), команда
контроль объекта 532, 564, 583
необходимые права доступа к объектам 491

CRTSSND (Создать описание сеанса), команда
необходимые права доступа к объектам 500

CRTTAPF (Создать файл магнитной ленты), команда
необходимые права доступа к объектам 408

CRTTBL (Создать таблицу), команда
необходимые права доступа к объектам 516

CRTTIMZON, команда 518

CRTUDFS
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CRTUDFS (Создать пользовательскую файловую систему), команда
необходимые права доступа к объектам 519
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CRTUSRPRF (Создать пользовательский профайл), команда
использование 123
необходимые права доступа к объектам 521
описание 329, 330

CRTVLDL (Создать контрольный список), команда
необходимые права доступа к объектам 523
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CRTWSCST (Создать объект настройки рабочей станции), команда
необходимые права доступа к объектам 523

cryptography
права доступа к объектам, необходимые для применения команд 388

CU (операции с кластерами), формат файла 622

CURLIB (текущая библиотека), параметр пользовательский профайл 85

CV (проверка соединения), формат файла 624

CVTBASSTR (Преобразовать потоковые файлы BASIC), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CVTBASUNF (Преобразовать неформатированные файлы BASIC), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CVTBGUDTA (Преобразовать данные BGU), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CVTCLSRC (Преобразовать исходный код на CL), команда
необходимые права доступа к объектам 491

CVTDIR
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CVTDIR (Преобразовать каталог), команда
необходимые права доступа к объектам 420

CVTEDU (Преобразовать обучение), команда
необходимые права доступа к объектам 477

CVTIPSIFC (Преобразовать интерфейс IP для SNA), команда
необходимые права доступа к объектам 373

CVTIPSLOC (Преобразовать запись о расположении IP для SNA), команда
необходимые права доступа к объектам 373

CVTOPTBKV (Преобразовать резервную копию оптического носителя), команда
необходимые права доступа к объектам 479

CVTPFRCOL (Преобразовать базу данных статистики), команда
необходимые права доступа к объектам 485
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CVTPFRDTA
пользовательские профайлы, поставляемые IBM, с правами доступа 350

CVTPFRDTA (Преобразовать базу данных статистики), команда
необходимые права доступа к объектам 485

CVTPFRTHD
пользовательские профайлы, поставляемые IBM, с правами доступа 351

CVTPFRTHD (Преобразовать базу данных статистики нити), команда
необходимые права доступа к объектам 485

CVTRJEDTA (Преобразовать данные RJE), команда
необходимые права доступа к объектам 500

CVTRPGSRC (Преобразовать исходный код RPG), команда
необходимые права доступа к объектам 455

CVTS36FCT (Преобразовать таблицу управления формами System/36), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 351

CVTS36JOB (Преобразовать задание System/36), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 351

CVTS38JOB (Преобразовать задание System/38), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 351

CVTSQCPP (Преобразовать исходный код SQL C++), команда
необходимые права доступа к объектам 455

CVTTCPCPL (Преобразовать команды TCP/IP), команда
необходимые права доступа к объектам 516

CVTTCPCPL (Преобразовать управляющий язык TCP/IP), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 351

CVTTOFLR (Преобразовать в папку), команда
контроль объекта 545

CY (настройка шифрования), формат файла 626

D

DB2LDIF, команда
необходимые права доступа к объектам 394

DCEADM (QDCEADM), пользовательский профайл 339

DCPOBJ (Развернуть объект), команда
контроль объекта 529
необходимые права доступа к объектам 365

DDM (управление распределенными данными)
защита 227

DDM, обработка запросов, сетевой атрибут DDMACC 227

DDMACC (доступ к DDM), сетевой атрибут 277

DDMACC (обработка запросов DDM), сетевой атрибут 227

DEV (принтер), параметр
пользовательский профайл 108

DI (Сервер каталогов), формат файла 629

DLCOBJ (Освободить объект), команда
контроль объекта 529
необходимые права доступа к объектам 365

DLO (объект библиотеки документов)
права доступа
описание команд 332

DLTADMDMN, команда
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTALR (Удалить предупреждение), команда
необходимые права доступа к объектам 373

DLTALRTBL (Удалить таблицу предупреждений), команда
необходимые права доступа к объектам 373

DLTAPARDTA (Удалить данные APAR), команда
необходимые права доступа к объектам 503
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTAUTHLR (Удалить владельца прав доступа), команда
использование 161
необходимые права доступа к объектам 375
описание 327, 332

DLTAUTL (Удалить список прав доступа), команда
использование 177
необходимые права доступа к объектам 376
описание 327

DLTBESTMDL (Удалить модель BEST/1), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTBESTMDL (Удалить модель Best/1-400), команда
необходимые права доступа к объектам 485

DLTBNDDIR (Удалить каталог связывания), команда
необходимые права доступа к объектам 376

DLTCFGL (Удалить список конфигурации), команда
необходимые права доступа к объектам 385

DLTCHTFMT (Удалить формат диаграммы), команда
необходимые права доступа к объектам 377

DLTCLD (Удалить описание локали C), команда
необходимые права доступа к объектам 456

DLTCLS (Удалить класс), команда
необходимые права доступа к объектам 378

DLTCLU
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTCLU, команда
необходимые права доступа к объектам 380

DLTCMD (Удалить команду), команда
необходимые права доступа к
объектам 382

DLTCMNTRC (Удалить данные
трассировки соединений), команда
необходимые права доступа к
объектам 503
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTCNNL (Удалить список соединений),
команда
необходимые права доступа к
объектам 385

DLTCOSD (Удалить описание класса
обслуживания), команда
необходимые права доступа к
объектам 378

DLTCRGCLU
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTCRQD (Удалить описание запроса на
изменение), команда
необходимые права доступа к
объектам 377

DLTCSI (Удалить исходную информацию
связи), команда
необходимые права доступа к
объектам 384

DLTCTLD (Удалить описание
контроллера), команда
необходимые права доступа к
объектам 387

DLTDEVD (Удалить описание устройства),
команда
контроля объекта 587
необходимые права доступа к
объектам 391

DLTDFUPGM (Удалить программу DFU),
команда
необходимые права доступа к
объектам 491

DLTDKTLBL (Удалить метку с дискеты),
команда
необходимые права доступа к
объектам 465

DLTDLO (Удалить объект библиотеки
документов), команда
контроля объекта 545
необходимые права доступа к
объектам 397

DLTDOCL (Удалить список документов),
команда
контроля объекта 545
необходимые права доступа к
объектам 397

DLTDST (Удалить рассылку), команда
контроля объекта 545
необходимые права доступа к
объектам 395

DLTDSTL (Удалить список рассылки),
команда
необходимые права доступа к
объектам 396

DLTDTAARA (Удалить область данных),
команда
необходимые права доступа к
объектам 389

DLTDTADCT (Удалить словарь данных),
команда
необходимые права доступа к
объектам 435

DLTDTAQ (Удалить очередь данных),
команда
необходимые права доступа к
объектам 390

DLTEDTD (Удалить описание формата),
команда
необходимые права доступа к
объектам 403

DLTEXPSPLF
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTF (Удалить файл), команда
необходимые права доступа к
объектам 408

DLTFCNARA
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTFCNARA (Удалить функциональную
область), команда
необходимые права доступа к
объектам 485

DLTFCT (Удалить таблицу управления
формами), команда
необходимые права доступа к
объектам 500

DLTFNTRSC (Удалить ресурсы шрифтов),
команда
необходимые права доступа к
объектам 372

DLTFNTTBL (Удалить таблицу шрифтов
DBCS)
права доступа к объектам,
необходимые для применения
команд 372

DLTFORMDF (Удалить определение
формы), команда
необходимые права доступа к
объектам 372

DLTFTR (Удалить фильтр), команда
необходимые права доступа к
объектам 412

DLTGPHFMT
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTGPHFMT (Удалить графический
формат), команда
необходимые права доступа к
объектам 485

DLTGPHPKG
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTGPHPKG (Удалить графический
пакет), команда
необходимые права доступа к
объектам 485

DLTGSS (Удалить набор графических
символов), команда
необходимые права доступа к
объектам 413

DLTHSTDTA
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTHSTDTA (Удалить данные
хронологии), команда
необходимые права доступа к
объектам 485

DLTIGCDCT (Удалить словарь
преобразования DBCS), команда
необходимые права доступа к
объектам 402

DLTIGCSRT (Удалить сортировку IGC),
команда
необходимые права доступа к
объектам 402

DLTIGCTBL (Удалить таблицу шрифтов
DBCS), команда
необходимые права доступа к
объектам 402

DLTIMGCLG, команда
необходимые права доступа к
объектам 414

DLTIPXD, команда 436

DLTJOB (Удалить описание задания),
команда
необходимые права доступа к
объектам 441

DLTJOBQ (Удалить очередь заданий),
команда
необходимые права доступа к
объектам 442

DLTJRN (Удалить журнал), команда
необходимые права доступа к
объектам 444

DLTJRNRCV (Удалить получатель
журнала), команда
выключение функции контроля 312
необходимые права доступа к
объектам 447

DLTLIB (Удалить библиотеку), команда
необходимые права доступа к
объектам 457

DLTLICPGM (Удалить лицензионную
программу), команда
необходимые права доступа к
объектам 461
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351

DLTLIND (Удалить описание линии),
команда
необходимые права доступа к
объектам 463

DLTLOCALE (Удалить локаль), команда
необходимые права доступа к
объектам 464

DLTMNU (Удалить меню), команда
необходимые права доступа к
объектам 466

DLTMOD (Удалить модуль), команда
необходимые права доступа к
объектам 470

DLTMODD (Удалить описание режима), команда
необходимые права доступа к объектам 469

DLTMSGF (Удалить файл сообщений), команда
необходимые права доступа к объектам 468

DLTMSGQ (Удалить очередь сообщений), команда
необходимые права доступа к объектам 468

DLTNETF (Удалить сетевой файл), команда
необходимые права доступа к объектам 471

DLTNODL (Удалить список узлов), команда
необходимые права доступа к объектам 476

DLTNTBD (Удалить описание NetBIOS), команда
необходимые права доступа к объектам 470

DLTNWID (Удалить описание сетевого интерфейса), команда
необходимые права доступа к объектам 473

DLTNWSALS (Удалить псевдоним сетевого сервера), команда
необходимые права доступа к объектам 474

DLTNWSCFG, команда
необходимые права доступа к объектам 475
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTNWSD (Удалить описание сетевого сервера), команда
необходимые права доступа к объектам 475

DLTNWSSTG (Удалить область памяти сетевого сервера), команда
необходимые права доступа к объектам 473

DLTOUTQ (Удалить очередь вывода), команда
необходимые права доступа к объектам 481

DLTOVL (Удалить перекрытие), команда
необходимые права доступа к объектам 372

DLTPAGDFN (Удалить определение страницы), команда
необходимые права доступа к объектам 372

DLTPAGSEG (Удалить сегмент страницы), команда
необходимые права доступа к объектам 372

DLTPDG (Удалить группу дескрипторов печати), команда
необходимые права доступа к объектам 489

DLTPREXDTA
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTPREXDTA (Удалить данные PEX), команда
необходимые права доступа к объектам 486

DLTPFCOL (Удалить базу данных статистики), команда
необходимые права доступа к объектам 486
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTPFRDTA
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTPFRDTA (Удалить базу данных статистики), команда
необходимые права доступа к объектам 486

DLTPGM (Удалить программу), команда
необходимые права доступа к объектам 491

DLTPNLGRP (Удалить группу панелей), команда
необходимые права доступа к объектам 466

DLTPRB (Удалить неполадку), команда
необходимые права доступа к объектам 489
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTPSFCFG (Удалить конфигурацию Print Services Facility), команда
необходимые права доступа к объектам 489

DLTPTF (Удалить PTF), команда
необходимые права доступа к объектам 503
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTQMFORM (Удалить форму управления запросами), команда
необходимые права доступа к объектам 494

DLTQMQRV (Удалить запрос на управление запросом), команда
необходимые права доступа к объектам 494

DLTQRY (Удалить запрос), команда
контроль объекта 576
необходимые права доступа к объектам 494

DLTQST (Удалить вопрос), команда
необходимые права доступа к объектам 495
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTQSTDB (Удалить базу данных вопросов и ответов), команда
необходимые права доступа к объектам 495
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTRJECFG (Удалить конфигурацию RJE), команда
необходимые права доступа к объектам 500

DLTRMPTPF (Удалить удаленный PTF), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTSBSD (Удалить описание подсистемы), команда
необходимые права доступа к объектам 511

DLTSCHIDX (Удалить индекс поиска), команда
необходимые права доступа к объектам 436

DLTSHF (Удалить книжную полку), команда
контроль объекта 545

DLTSMGOBJ (Удалить объект управления системами), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 351

DLTSPADCT (Удалить орфографический словарь), команда
необходимые права доступа к объектам 507

DLTSPLF (Удалить буферный файл), команда
действие, контроль 582
контроль объекта 569
необходимые права доступа к объектам 509

DLTSQLPKG (Удалить пакет языка структурных запросов), команда
необходимые права доступа к объектам 482

DLTSRVPGM (Удалить служебную программу), команда
необходимые права доступа к объектам 491

DLTSSND (Удалить описание сеанса), команда
необходимые права доступа к объектам 500

DLTTBL (Удалить таблицу), команда
необходимые права доступа к объектам 516

DLTTIMZON, команда 518

DLTTRC (Удалить данные трассировки), команда
необходимые права доступа к объектам 503

DLTUDFS (Удалить пользовательскую файловую систему), команда
необходимые права доступа к объектам 519

- DLTUDFS (Удалить пользовательскую файловую систему), команда
(*продолжение*)
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DLTUSRIDX (Удалить пользовательский индекс), команда
необходимые права доступа к
объектам 518
- DLTUSRPRF (Удалить пользовательский профайл), команда
контроля объекта 589
необходимые права доступа к
объектам 521
описание 330
пример 127
принадлежность объекта 150
- DLTUSRQ (Удалить пользовательскую очередь), команда
необходимые права доступа к
объектам 518
- DLTUSRSPC (Удалить пользовательское пространство индекса), команда
необходимые права доступа к
объектам 518
- DLTUSRTRC (Удалить пользовательскую трассировку), команда
необходимые права доступа к
объектам 438
- DLTVLDL (Удалить контрольный список), команда
необходимые права доступа к
объектам 523
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DLTWNTSVR, команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DLTWSCST (Удалить объект настройки рабочей станции), команда
необходимые права доступа к
объектам 523
- DLVRY (доставка в очередь сообщений), параметр
пользовательский профайл 107
- DLYJOB (Отложить задание), команда
необходимые права доступа к
объектам 438
- DMPCLPGM (Создать дампы программы на CL), команда
контроля объекта 572
необходимые права доступа к
объектам 491
- DMPDLO (Создать дампы объектов библиотеки документов), команда
контроля объекта 544
необходимые права доступа к
объектам 397
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPJOB (Создать дампы задания), команда
необходимые права доступа к
объектам 503
- DMPJOB (Создать дампы задания), команда
(*продолжение*)
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPJOBINT (Создать внутренний дампы задания), команда
необходимые права доступа к
объектам 503
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPJVM
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPMEMINF
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPOBJ (Создать дампы объектов), команда
контроля объекта 527
необходимые права доступа к
объектам 365
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPYSOBY (Создать дампы системного объекта), команда
контроля объекта 527
необходимые права доступа к
объектам 365
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPYAP (Создать дампы магнитной ленты), команда
необходимые права доступа к
объектам 465
- DMPTRC (Создать дампы трассировки), команда
необходимые права доступа к
объектам 486
пользовательские профайлы,
поставляемые IBM, с правами
доступа 351
- DMPUSRPRF (Создать дампы пользовательского профайла), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 352
- DMPUSRTRC (Создать дампы пользовательской трассировки), команда
необходимые права доступа к
объектам 438
- DO (операция удаления), тип записи журнала 288
- DO (операция удаления), формат файла 635
- DOCPWD (пароль документа), параметр
пользовательский профайл 106
- DS (сброс пароля DST), тип записи журнала 294
- DS (сброс поставляемого IBM ИД пользователя сервисных средств), формат файла 637
- DSCJOB (Отсоединить задание), команда
необходимые права доступа к
объектам 438
- DSPACC (Показать код доступа), команда
контроля объекта 547
необходимые права доступа к
объектам 476
- DSPACCAUT (Показать права кода доступа), команда
необходимые права доступа к
объектам 476
- DSPACTPJ (Показать активные предварительные задания), команда
необходимые права доступа к
объектам 438
- DSPACTPRFL (Показать список активных профайлов), команда
необходимые права доступа к
объектам 521
описание 749
- DSPACTSCD (Показать расписание активации), команда
необходимые права доступа к
объектам 521
описание 749
- DSPASPSTS, команда
необходимые права доступа к
объектам 391
- DSPAUDJRNE (Показать записи журнала контроля), команда
необходимые права доступа к
объектам 444
описание 334, 754
- DSPAUT (Показать права доступа), команда
контроля объекта 542, 580, 585
необходимые права доступа к
объектам 420
описание 328
- DSPAUTHLR (Показать владельца прав доступа), команда
использование 160
контроля объекта 532
необходимые права доступа к
объектам 375
описание 327
- DSPAUTL (Показать список прав доступа), команда
контроля объекта 531
необходимые права доступа к
объектам 376
описание 327
- DSPAUTLDLO (Показать объекты библиотеки документов из списка прав доступа), команда
контроля объекта 531
необходимые права доступа к
объектам 376, 397
описание 332
- DSPAUTLJOB (Показать объекты списка прав доступа), команда
использование 176
контроля объекта 531
необходимые права доступа к
объектам 376
описание 327

DSPAUTUSR (Показать пользователей с правами доступа), команда
необходимые права доступа к объектам 521
описание 330
параметров контроля 320
пример 130

DSPBCKSTS (Показать состояние резервного копирования), команда
необходимые права доступа к объектам 477

DSPBCKUP (Показать опции резервного копирования), команда
необходимые права доступа к объектам 477

DSPBCKUPL (Показать список резервного копирования), команда
необходимые права доступа к объектам 477

DSPBCKP (Показать точки прерывания), команда
необходимые права доступа к объектам 491

DSPBNDDIR (Показать каталог связывания), команда
необходимые права доступа к объектам 376

DSPBNDDIRE (Показать каталог связывания), команда
контроля объекта 532

DSPCDEFNT (Показать кодированный шрифт)
права доступа к объектам,
необходимые для применения команд 372

DSPCFGL (Показать список конфигурации), команда
контроля объекта 533
необходимые права доступа к объектам 385

DSPCHT (Показать диаграмму), команда
контроля объекта 533
необходимые права доступа к объектам 377

DSPCKMKSFE, команда
необходимые права доступа к объектам 388

DSPCLS (Показать класс), команда
контроля объекта 535
необходимые права доступа к объектам 378

DSPCMD (Показать команду), команда
контроля объекта 535
необходимые права доступа к объектам 382

DSPCNNL (Показать список соединений), команда
контроля объекта 536
необходимые права доступа к объектам 385

DSPCNNSTS (Показать состояние соединения), команда
необходимые права доступа к объектам 391

DSPCOSD (Показать описание класса обслуживания), команда
контроля объекта 537

DSPCOSD (Показать описание класса обслуживания), команда (*продолжение*)
необходимые права доступа к объектам 378

DSPCPCST (Показать ограничения, ожидающие проверки), команда
контроля объекта 553
необходимые права доступа к объектам 409

DSPCSI (Показать исходную информацию связи), команда
контроля объекта 537
необходимые права доступа к объектам 384

DSPCSPOBJ (Показать объект CSP/AE), команда
контроля объекта 537, 538, 572

DSPCTLD (Показать описание контроллера), команда
контроля объекта 538
необходимые права доступа к объектам 387

DSPCURDIR (Показать текущий каталог), команда
контроля объекта 540
необходимые права доступа к объектам 420

DSPDBG (Показать данные отладки), команда
необходимые права доступа к объектам 491

DSPDBGWCH (Показать условия отслеживания отладки), команда
необходимые права доступа к объектам 491

DSPDBR (Показать отношения базы данных), команда
контроля объекта 553
необходимые права доступа к объектам 409

DSPDDMF (Показать файл Управления распределенными данными), команда
необходимые права доступа к объектам 409

DSPDEV (Показать описание устройства), команда
контроля объекта 539
необходимые права доступа к объектам 391

DSPDIRE (Показать запись каталога), команда
необходимые права доступа к объектам 393

DSPDKT (Показать содержимое дискеты), команда
необходимые права доступа к объектам 465

DSPDLOAUD (Показать параметры контроля объекта библиотеки документов), команда
использование 306
контроля объекта 544
необходимые права доступа к объектам 397
описание 332

DSPDLOAUT (Показать права доступа к объекту библиотеки документов), команда
контроля объекта 544
необходимые права доступа к объектам 397
описание 332

DSPDLONAM (Показать имя объекта библиотеки документов), команда
необходимые права доступа к объектам 397

DSPDOC (Показать документ), команда
контроля объекта 544
необходимые права доступа к объектам 397

DSPDSTL (Показать список рассылки), команда
необходимые права доступа к объектам 396

DSPDSTLOG (Показать протокол рассылки), команда
необходимые права доступа к объектам 395
пользовательские профайлы,
поставляемые IBM, с правами доступа 352

DSPDSTSRV (Показать службы рассылок), команда
необходимые права доступа к объектам 395

DSPDTA (Показать данные), команда
необходимые права доступа к объектам 409

DSPDTA (показать данные), параметр 222

DSPDTAARA (Показать область данных), команда
контроля объекта 547
необходимые права доступа к объектам 389

DSPDTADCT (Показать словарь данных), команда
необходимые права доступа к объектам 435

DSPEDTD (Показать описание формата), команда
контроля объекта 549
необходимые права доступа к объектам 403

DSPWCBCDE (Показать запись штрихового кода для контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 404

DSPWCM (Показать элемент контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 404

DSPWCPTCE (Показать запись PTC контроллера расширенной беспроводной сети), команда
необходимые права доступа к объектам 404

DSPPEWLM (Показать элемент линии расширенной беспроводной сети), команда
необходимые права доступа к объектам 404

DSPPEXPSCD (Показать расписание истечения срока), команда
необходимые права доступа к объектам 521
описание 749

DSPPF (Показать файл), команда 421

DSPFPD (Показать описание файла), команда
контроля объекта 553
необходимые права доступа к объектам 409

DSPFFD (Показать описание полей файла), команда
контроля объекта 553
необходимые права доступа к объектам 409

DSPFLR (Показать папку), команда
необходимые права доступа к объектам 397

DSPFNTRSCA (Показать атрибуты ресурса шрифта), команда
необходимые права доступа к объектам 373

DSPFNTTBL (Показать таблицу шрифтов DBCS)
права доступа к объектам, необходимые для применения команд 373

DSPGDF (Показать файл графических данных), команда
необходимые права доступа к объектам 377

DSPHDWRSC (Показать аппаратные ресурсы), команда
необходимые права доступа к объектам 497

DSPHLPDOC (Показать справочный документ), команда
контроля объекта 544

DSPHSTGPH
пользовательские профайлы, поставляемые IBM, с правами доступа 352

DSPHSTGPH (Показать графическое представление хронологии), команда
необходимые права доступа к объектам 486

DSPIGCDCT (Показать словарь преобразования DBCS), команда
контроля объекта 556
необходимые права доступа к объектам 402

DSPIPXD, команда 436

DSPJOB (Показать задание), команда
необходимые права доступа к объектам 438

DSPJOB (Показать описание задания), команда
использование 276
контроля объекта 557
необходимые права доступа к объектам 441

DSPJOBLOG (Показать протокол задания), команда
необходимые права доступа к объектам 438

DSPJRN (Показать журнал), команда
контроль операций с файлами 248, 319
контроля объекта 559, 560
необходимые права доступа к объектам 445
пример журнала контроля (QAUDJRN) 313, 314
просмотр QAUDJRN (журнала контроля) 278
создание файла вывода 315

DSPJRNA (S/38E) Работа с атрибутами журнала
контроля объекта 560

DSPJRNNU (S/38E) Работа с журналом контроля объекта 560

DSPJRNRCVA (Показать атрибуты получателя журнала), команда
контроля объекта 560
необходимые права доступа к объектам 448

DSPJVMJOB, команда
необходимые права доступа к объектам 437

DSPLANADPP (Показать профайл адаптера LAN), команда
необходимые права доступа к объектам 464

DSPLANSTS (Показать состояние локальной сети), команда
необходимые права доступа к объектам 464

DSPLIB (Показать библиотеку), команда
использование 321
контроля объекта 561
необходимые права доступа к объектам 457

DSPLIBD (Показать описание библиотеки), команда
CRTAUT, параметр 165
необходимые права доступа к объектам 457

DSPLOCKEY (Показать ключ лицензии), команда
необходимые права доступа к объектам 461

DSPLIND (Показать описание линии), команда
контроля объекта 562
необходимые права доступа к объектам 463

DSPLNK
необходимые права доступа к объектам 421

DSPLNK (Показать связи), команда
контроля объекта 540, 579, 584, 586

DSPLOG (Показать протокол), команда
контроля объекта 565
необходимые права доступа к объектам 468

DSPMFSINF (Показать информацию о смонтированной файловой системе), команда
необходимые права доступа к объектам 472

DSPMGDSYSA (Показать атрибуты управляемой системы), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

DSPMNUA (Показать атрибуты меню), команда
контроля объекта 563
необходимые права доступа к объектам 466

DSPMOD (Показать модуль), команда
контроля объекта 564
необходимые права доступа к объектам 470

DSPMODD (Показать описание режима), команда
контроля объекта 564
необходимые права доступа к объектам 469

DSPMODSRC (Показать исходный код модуля), команда
контроля объекта 551
необходимые права доступа к объектам 491

DSPMODSTS (Показать состояние режима), команда
контроля объекта 539
необходимые права доступа к объектам 469

DSPMSG (Показать сообщения), команда
контроля объекта 565
необходимые права доступа к объектам 467

DSPMSGD (Показать описания сообщений), команда
контроля объекта 564
необходимые права доступа к объектам 467

DSPNETA (Показать сетевые атрибуты), команда
необходимые права доступа к объектам 471

DSPNTBD (Показать описание NetBIOS), команда
контроля объекта 567
необходимые права доступа к объектам 471

DSPNWID (Показать описание сетевого интерфейса), команда
контроля объекта 567
необходимые права доступа к объектам 473

DSPNWSA (Показать атрибут сетевого сервера), команда
необходимые права доступа к объектам 474

DSPNWSALS (Показать псевдоним сетевого сервера), команда
необходимые права доступа к объектам 474

DSPNWSCFG, команда
необходимые права доступа к
объектам 475
пользовательские профайлы,
поставляемые IBM, с правами
доступа 352

DSPNWSD (Показать описание сетевого
сервера), команда
контроля объекта 568
необходимые права доступа к
объектам 475

DSPNWSSSN (Показать сеанс сетевого
сервера), команда
необходимые права доступа к
объектам 474

DSPNWSSTC (Показать статистику для
сетевого сервера), команда
необходимые права доступа к
объектам 474

DSPNWSSTG (Показать область памяти
сетевого сервера), команда
необходимые права доступа к
объектам 474

DSPNWSUSR (Показать пользователя
сетевого сервера), команда
необходимые права доступа к
объектам 474

DSPNWSUSRA (Показать атрибут
пользователя сетевого сервера), команда
необходимые права доступа к
объектам 474

DSPOBJAUT (Показать права доступа к
объекту), команда
использование 321
контроля объекта 529
необходимые права доступа к
объектам 365
описание 328

DSPOBJD (Показать описание объекта),
команда
использование 306
контроля объекта 529
необходимые права доступа к
объектам 365
описание 328
с помощью файла вывода 321
создан 151

DSPOPT (Показать оптический
накопитель), команда
необходимые права доступа к
объектам 479

DSPOPTLCK (Показать блокировку
оптического накопителя), команда
необходимые права доступа к
объектам 479

DSPORTSVR (Показать сервер оптических
накопителей), команда
необходимые права доступа к
объектам 479

DSPPDGPRF (Показать профайл группы
дескрипторов печати), команда
необходимые права доступа к
объектам 489

DSPPFM (Показать элемент физического
файла), команда
контроля объекта 550

DSPPFM (Показать элемент физического
файла), команда (*продолжение*)
необходимые права доступа к
объектам 409

DSPPFDRDTA
пользовательские профайлы,
поставляемые IBM, с правами
доступа 352

DSPPFDRDTA (Показать базу данных
статистики), команда
необходимые права доступа к
объектам 486

DSPPFGRPH
пользовательские профайлы,
поставляемые IBM, с правами
доступа 352

DSPPFGRPH (Показать графическое
представление статистики), команда
необходимые права доступа к
объектам 486

DSPPGM (Показать программу), команда
контроля объекта 572
необходимые права доступа к
объектам 491
принятые права доступа 159
режим программы 16

DSPPGMADP (Показать принимающие
программы), команда
использование 159, 248
контроля объекта 589
необходимые права доступа к
объектам 521
описание 331
параметров контроля 322

DSPPGMREF (Показать ссылки на
программу), команда
контроля объекта 553
необходимые права доступа к
объектам 491

DSPPGMVAR (Показать переменную
программы), команда
необходимые права доступа к
объектам 491

DSPPRB (Показать неполадку), команда
необходимые права доступа к
объектам 489

DSPPTF (Показать временное исправление
программы), команда
необходимые права доступа к
объектам 503
пользовательские профайлы,
поставляемые IBM, с правами
доступа 352

DSPPWSCD (Показать расписание
включения и выключения питания),
команда
необходимые права доступа к
объектам 477

DSPRCYAP (Показать параметры
восстановления путей доступа), команда
контроля объекта 530
необходимые права доступа к
объектам 372

DSPRDBDIRE (Показать запись каталога
реляционной базы данных), команда
необходимые права доступа к
объектам 497

DSPRJECFG (Показать конфигурацию
RJE), команда
необходимые права доступа к
объектам 500

DSPS36 (Показать System/36), команда
контроля объекта 587
необходимые права доступа к
объектам 514

DSPSAVF (Показать файл сохранения),
команда
необходимые права доступа к
объектам 409

DSPSBSDD (Показать описание
подсистемы), команда
контроля объекта 578
необходимые права доступа к
объектам 511

DSPSECA (Показать атрибуты защиты),
команда
необходимые права доступа к
объектам 502

DSPSECAUD (Показать значения
контроля за действиями), команда
необходимые права доступа к
объектам 502
описание 334

DSPSECAUD (Показать параметры
контроля действий), команда
описание 751

DSPSFWRSC (Показать программные
ресурсы), команда
необходимые права доступа к
объектам 497

DSPSGNINF (показать информацию о
входе в систему), параметр
пользовательский профайл 96

DSPSOCSTS (Показать состояние сферы
управления), команда
необходимые права доступа к
объектам 507

DSPSPLF (Показать буферный файл),
команда
DSPDTA, параметр очереди
вывода 222
действие, контроль 581
контроля объекта 569
необходимые права доступа к
объектам 509

DSPSRVA (Показать служебные
атрибуты), команда
необходимые права доступа к
объектам 503

DSPSRVPGM (Показать служебную
программу), команда
контроля объекта 583
необходимые права доступа к
объектам 492
принятые права доступа 159

DSPSRVSTS (Показать состояние службы),
команда
необходимые права доступа к
объектам 503
пользовательские профайлы,
поставляемые IBM, с правами
доступа 352

- DSPSSSTUSR (Показать ИД пользователя сервисных средств), команда
необходимые права доступа к объектам 503
- DSPSSSTUSR, команда
необходимые права доступа к объектам 521
- DSPSYSSTS (Показать состояние системы), команда
необходимые права доступа к объектам 512
- DSPSYSVAL (Показать системное значение), команда
необходимые права доступа к объектам 513
- DSPTAP (Показать содержимое магнитной ленты), команда
необходимые права доступа к объектам 465
- DSPTAPCTG (Показать кассету магнитной ленты), команда
необходимые права доступа к объектам 465
- DSPTRC (Показать трассировку), команда
необходимые права доступа к объектам 492
- DSPTRCDDTA (Показать данные трассировки), команда
необходимые права доступа к объектам 492
- DSPUDFS (Показать пользовательскую файловую систему), команда
необходимые права доступа к объектам 519
- DSPUSRPMN (Показать права доступа пользователя), команда
контроль объекта 547
необходимые права доступа к объектам 476
- DSPUSRPRF (Показать пользовательский профайл), команда
использование 130
контроль объекта 589
необходимые права доступа к объектам 521
описание 330
с помощью файла вывода 320
- DSPVTMAP (Показать раскладку клавиатуры VT100), команда
необходимые права доступа к объектам 517
- DST (специальные сервисные средства)
изменение ИД пользователя 135
изменение паролей 135
контроль паролей 273
сброс пароля
запись журнала контроля (QAUDJRN) 294
описание команды 329
- DUPDKT (Дублировать дискету), команда
необходимые права доступа к объектам 465
- DUPORT (Скопировать оптический том), команда
необходимые права доступа к объектам 479
- DUPTAP (Дублировать магнитную ленту), команда
необходимые права доступа к объектам 465
- ## E
- EDTAUTL (Редактировать список прав доступа), команда
использование 175
контроль объекта 531
необходимые права доступа к объектам 376
описание 327
- EDTBCKUPL (Изменить список резервного копирования), команда
необходимые права доступа к объектам 477
- EDTGPCST (Изменить ограничения, ожидающие проверки), команда
контроль объекта 553
необходимые права доступа к объектам 409
пользовательские профайлы, поставляемые IBM, с правами доступа 352
- EDTDEVRSC (Изменить ресурсы устройства), команда
необходимые права доступа к объектам 497
- EDTDLOAUT (Редактировать права доступа к объекту библиотеки документов), команда
контроль объекта 544, 545
необходимые права доступа к объектам 397
описание 332
- EDTDOC (Редактировать документ), команда
контроль объекта 546
необходимые права доступа к объектам 397
- EDTF (Редактировать файл), команда 424
- EDTIGCDCT (Редактировать словарь преобразования DBCS), команда
контроль объекта 556
необходимые права доступа к объектам 402
- EDTLIBL (Изменить список библиотек), команда
использование 218
необходимые права доступа к объектам 457
- EDTOBJAUT (Редактировать права доступа к объекту), команда
использование 167
контроль объекта 530
необходимые права доступа к объектам 365
описание 328
- EDTQST (Редактировать вопросы и ответы), команда
необходимые права доступа к объектам 495
- EDTQST (Редактировать вопросы и ответы), команда (*продолжение*)
пользовательские профайлы, поставляемые IBM, с правами доступа 352
- EDTRBDAP (Изменить параметры реорганизации путей доступа), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352
- EDTRCYAP (Редактировать восстановление путей доступа), команда
контроль объекта 530
необходимые права доступа к объектам 372
пользовательские профайлы, поставляемые IBM, с правами доступа 352
- EDTS36PGMA (Редактировать атрибуты программы System/36), команда
контроль объекта 572
необходимые права доступа к объектам 514
- EDTS36PRCA (Редактировать атрибуты процедуры System/36), команда
контроль объекта 552
необходимые права доступа к объектам 515
- EDTS36SRCA (Редактировать атрибуты исходного текста System/36), команда
контроль объекта 552
необходимые права доступа к объектам 515
- EDTWSOAUT (Изменить права доступа к объекту рабочей станции), команда
необходимые права доступа к объектам 412
- EIMASSOC (связь eim), параметр пользовательский профайл 115
- EJTEMLOUT (Извлечь вывод эмуляции), команда
необходимые права доступа к объектам 392
- EML3270 (Эмулировать дисплей 3270), команда
необходимые права доступа к объектам 393
- EMLPRTKEY (Эмулировать ключ принтера), команда
необходимые права доступа к объектам 392
- ENCCPHK (Зашифровать ключ шифрования), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 352
- ENCFRMMSTK (Зашифровать исходный главный ключ), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENCTOMSTK (Зашифровать целевой главный ключ), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDASPBAL
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDASPBAL, команда 392

ENDCBLDBG (Завершить отладку COBOL), команда
необходимые права доступа к объектам 456, 492

ENDCHTSVR
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDCLNUP (Завершить очистку), команда
необходимые права доступа к объектам 477

ENDCLUNOD
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDCLUNOD, команда
необходимые права доступа к объектам 381

ENDCMNTRC
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDCMNTRC (Завершить трассировку соединений), команда
необходимые права доступа к объектам 503

ENDCMTCTL (Завершить управление фиксацией), команда
необходимые права доступа к объектам 383

ENDCPYSCN (Завершить копирование экрана), команда
необходимые права доступа к объектам 503

ENDCRG
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDCTLRCY (Прекратить исправление ошибок контроллера), команда
контроль объекта 538
необходимые права доступа к объектам 387

ENDDBG (Закончить отладку), команда
необходимые права доступа к объектам 492

ENDDBGSVR (Остановить сервер отладки), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDDBMON (Выключить монитор баз данных), команда
необходимые права доступа к объектам 488

ENDDEVRCY (Прекратить исправление ошибок устройства), команда
контроль объекта 539
необходимые права доступа к объектам 392

ENDDIRSHD (Закончить работу с теневыми каталогами), команда
необходимые права доступа к объектам 393

ENDDIRSHD (Прекратить теневое копирование каталога), команда
контроль объекта 543

ENDDSKRGZ (Завершить реорганизацию диска), команда
необходимые права доступа к объектам 394

ENDDDW, команда
необходимые права доступа к объектам 486
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDGRPJOB (Завершить групповое задание), команда
необходимые права доступа к объектам 438

ENDHOSTSVR
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDHOSTSVR (Завершить работу сервера хоста), команда
необходимые права доступа к объектам 413

ENDIDXMOM (Остановить монитор индекса), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDIPSIFC (Завершить работу интерфейса IP для SNA), команда
необходимые права доступа к объектам 373
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDJOB (Завершить задание), команда
QINACTMSGQ, системное значение 30
действие, контроль 582
необходимые права доступа к объектам 438

ENDJOBABN (Завершить задание аварийно), команда
необходимые права доступа к объектам 438
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDJOBTRC
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDJOBTRC (Закончить трассировку задания), команда
необходимые права доступа к объектам 486

ENDJRN (Завершить ведение журнала), команда
контроль объекта 528
необходимые права доступа к объектам 424, 445

ENDJRNP (Завершить ведение журнала пути доступа), команда
необходимые права доступа к объектам 445

ENDJRNLIB (Завершить журналирование библиотеки), команда
необходимые права доступа к объектам 445

ENDJRNPF (Завершить ведение журнала физического файла), команда
необходимые права доступа к объектам 445

ENDJRNxxx (Завершить ведение журнала), команда
контроль объекта 559

ENDJW, команда
необходимые права доступа к объектам 486
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDLINRCY (Прекратить исправление ошибок линии), команда
контроль объекта 562
необходимые права доступа к объектам 463

ENDLOGSVR (Завершить работу сервера протокола задания), команда
необходимые права доступа к объектам 438

ENDMGDSYS (Завершить работу управляемой системы), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDMGRSRV (Остановить службы управления), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDMOD (Выключить режим), команда
контроль объекта 564
необходимые права доступа к объектам 469

ENDMSF (Завершить работу среды почтового сервера), команда
необходимые права доступа к объектам 464
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDNFSSVR (Завершить работу сервера NFS), команда
необходимые права доступа к объектам 472
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDNWIRCY (Прекратить исправление ошибок сетевого интерфейса), команда
контроль объекта 568

ENDPASTHR (Завершить сеанс удаленного входа), команда
необходимые права доступа к объектам 395

ENDPEX (Завершить работу PEX), команда
необходимые права доступа к объектам 486
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDPFRMON (Выключить монитор сбора статистики), команда
необходимые права доступа к объектам 488

ENDPFRTRC (Остановить трассировку производительности), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDPJ (Завершить работу предварительного задания), команда
действие, контроль 582
необходимые права доступа к объектам 438

ENDPRTEML (Завершить эмуляцию принтера), команда
необходимые права доступа к объектам 392

ENDRDR (Завершить чтение), команда
необходимые права доступа к объектам 496

ENDRJESSN (Завершить сеанс RJE), команда
необходимые права доступа к объектам 500

ENDRQS (Завершить запрос), команда
необходимые права доступа к объектам 492

ENDS36 (Завершить работу System/36), команда
контроль объекта 588

ENDSRVJOB (Завершить служебное задание), команда
необходимые права доступа к объектам 503
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDSYS (Завершить работу системы), команда
необходимые права доступа к объектам 512

ENDSYSMGR (Завершить работу System Manager), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDTCP (Завершить работу TCP/IP), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDTCPNN (Завершить соединение TCP/IP), команда
ENDTCP (Завершить работу TCP/IP), команда
необходимые права доступа к объектам 517

ENDTCPICF (Завершить интерфейс TCP/IP), команда
необходимые права доступа к объектам 517
необходимые права доступа к объектам 517
пользовательские профайлы, поставляемые IBM, с правами доступа 352

ENDTCPICF
пользовательские профайлы, поставляемые IBM, с правами доступа 353

ENDTCPPTP (Завершить двухточечный TCP/IP), команда
необходимые права доступа к объектам 516

ENDTCPSPRV (Остановить сервер TCP/IP), команда
необходимые права доступа к объектам 516

ENDTCPSPVR (Остановить сервер TCP/IP), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 353

ENDTRC (Завершить трассировку), команда
необходимые права доступа к объектам 503

ENDWCH (Завершить слежение), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 353

ENDWCH, команда
необходимые права доступа к объектам 503

ENDWTR (Завершить работу загрузчика), команда
необходимые права доступа к объектам 524

ENTCBLDBG (Включить отладку COBOL), команда
необходимые права доступа к объектам 456, 492

EV (переменная среды), формат файла 638

EXTPGMINF (Получить информацию о программе), команда
необходимые права доступа к объектам 492

F

faccessx (Определить доступные файлы для класса пользователей по дескриптору), команда
контроль объекта 540

FILDOC (Зарегистрировать документ), команда
контроль объекта 546

FILDOC (Зарегистрировать документ), команда (*продолжение*)
необходимые права доступа к объектам 397

FNDSTRPDM (Найти строку с помощью PDM), команда
необходимые права доступа к объектам 374

FTP (Протокол передачи файлов), команда
необходимые права доступа к объектам 516

G

GENCAT (Вставить каталог сообщений), команда
необходимые права доступа к объектам 409

GENCKMKSFE, команда
необходимые права доступа к объектам 388

GENCMDDOC (Создать документацию по командам), команда
необходимые права доступа к объектам 383

GENCPHK (Создать ключ шифрования), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 353

GENCRSDMNK (Создать междоменный ключ шифрования ключа), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 353

GENJVM DMP, команда
необходимые права доступа к объектам 437

GENMAC (Сгенерировать MAC), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 353

GENPIN (Сгенерировать PIN), команда
необходимые права доступа к объектам 388
пользовательские профайлы, поставляемые IBM, с правами доступа 353

GENS36RPT (Создать отчет System/36), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 353

GENS38RPT (Создать отчет System/38), команда
необходимые права доступа к объектам 469

GENS38RPT (Создать отчет System/38), команда *(продолжение)*
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

gid (номера ИД группы)
 восстановление 263

GO (Перейти к меню), команда
 необходимые права доступа к объектам 466

GR (шаблон записи), формат файла 639

GRPAUT (права доступа группы), параметр
 пользовательский профайл 103, 150, 152

GRPAUTTYPE (тип прав доступа группы), параметр
 пользовательский профайл 104, 152

GRPPRF (профайл группы), параметр
 пользовательский профайл описание 102
 пример 152

GRTACCAUT (Предоставить права доступа к коду доступа), команда
 контроля объекта 546
 необходимые права доступа к объектам 476
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

GRTOBJAUT (Предоставить права доступа к объекту), команда 167
 влияние на существующие права доступа 170
 контроля объекта 528
 необходимые права доступа к объектам 365
 несколько объектов 169
 описание 328

GRTUSRAUT (Предоставить пользователю права доступа), команда
 контроля объекта 589
 копирование прав доступа 127
 необходимые права доступа к объектам 521
 описание 330
 переименование профайла 132
 рекомендации 173

GRTUSRPMN (Предоставить права доступа пользователю), команда
 контроля объекта 546
 необходимые права доступа к объектам 476
 описание 332

GRTWSOAUT (Предоставить права доступа к объекту рабочей станции), команда
 необходимые права доступа к объектам 412

GS (задание дескриптора), тип записи журнала 298

GS (предоставить дескриптор), формат файла 644

H

HLDCMNDEV (Блокировать устройство связи), команда
 контроля объекта 539
 необходимые права доступа к объектам 392
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

HLDDSTQ (Блокировать очередь рассылки), команда
 необходимые права доступа к объектам 395
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

HLDJOB (Блокировать задание), команда
 необходимые права доступа к объектам 438

HLDJOBQ (Блокировать очередь заданий), команда
 контроля объекта 557
 необходимые права доступа к объектам 442

HLDJOBSCDE (Блокировать запись расписания заданий), команда
 контроля объекта 558
 необходимые права доступа к объектам 443

HLDOUTQ (Блокировать очередь вывода), команда
 контроля объекта 569
 необходимые права доступа к объектам 481

HLDRDR (Блокировать программу чтения), команда
 необходимые права доступа к объектам 496

HLDSPLF (Блокировать буферный файл), команда
 действие, контроль 582
 контроля объекта 569
 необходимые права доступа к объектам 509

HLDWTR (Блокировать загрузчик), команда
 необходимые права доступа к объектам 524

HOMEDIR (домашний каталог), параметр
 пользовательский профайл 115

I

IBM, поставляемые объекты
 защита с помощью списка прав доступа 145

INCLUDE, команда
 необходимые права доступа к объектам 456

INLMNU (начальное меню), параметр
 пользовательский профайл 87

INLPGM (начальная программа), параметр
 изменение 86
 пользовательский профайл 86

INSPTF (Установить временное исправление программы), команда
 необходимые права доступа к объектам 504
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

INSRMTPRD (Установить удаленный продукт), команда
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

INSWNTSVR, команда
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

INZDKT (Инициализировать дискету), команда
 необходимые права доступа к объектам 465

INZDSTQ (Инициализировать очередь рассылки), команда
 необходимые права доступа к объектам 395
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

INZNWSCFG, команда
 необходимые права доступа к объектам 475
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

INZOPT (Инициализировать оптический носитель), команда
 необходимые права доступа к объектам 480

INZPFM (Инициализировать элемент физического файла), команда
 контроля объекта 552
 необходимые права доступа к объектам 409

INZSYS (Инициализировать систему), команда
 необходимые права доступа к объектам 461
 пользовательские профайлы, поставляемые IBM, с правами доступа 353

INZTAP (Инициализировать магнитную ленту), команда
 необходимые права доступа к объектам 465

IP (действия по обмену данными между процессами), формат файла 648

IP (изменение принадлежности), тип записи 298

IP (межпроцессорная связь), тип записи журнала 287

IPL (Загрузка начальной программы)
 *JOBCTL (управление заданиями), специальные права доступа 91

IR (действия правил обработки пакетов IP), формат файла 649

IS (управление защитой в Internet), формат файла 651

iSeries Access
виртуальный принтер, защита 227
обмен сообщениями, защита 227
общая папка, защита 227
управление входом в систему 35
файл, передача, защита 227

J

Java
права доступа к объектам,
необходимые для применения
команд 437

JD (изменение описания задания), тип
записи журнала 298

JD (изменение описания задания), формат
файла 654

JKL Toys, компания
диаграмма приложений 231

job
*JOBCTL (управление заданиями),
специальные права доступа 91
автоматическая отмена 42, 45
выполнение только в пакетном
режиме 229
защита при запуске 209
изменение
запись журнала контроля
(QAUDJRN) 289
принятые права доступа 158
неактивный
тайм-аут (QINACTITV), системное
значение 29
планирование 229
права доступа к объектам,
необходимые для применения
команд 437
системное значение Проверять объект
при восстановлении
(QVfyOBRST) 45
тайм-аут для отключенного задания
(QDSCJOBITV), системное
значение 42

JOBACN (действие над заданием), сетевой
атрибут 225, 277

JOB D (описание задания), параметр
пользовательский профайл 101

JRNAP (Занести в журнал путь доступа),
команда
необходимые права доступа к
объектам 445

JRNAP (Начать ведение журнала пути
доступа), команда
контроля объекта 559

JRNPF (Занести в журнал физический
файл), команда
необходимые права доступа к
объектам 445

JRNPF (Начать ведение журнала
физического файла), команда
контроля объекта 559

JS (изменение задания), тип записи
журнала 289

JS (изменение задания), формат
файла 655

K

Kerberos
права доступа к объектам,
необходимые для применения
команд 448

KF (файл набора ключей), формат
файла 659

L

LANGID (идентификатор языка), параметр
SRTSEQ пользовательский профайл,
параметр 110
пользовательский профайл 111

LCLP WDMGT (локальное управление
паролем), параметр 97

LD (создание и удаление связей, поиск в
каталоге), формат файла 663

LDIF2DB, команда
необходимые права доступа к
объектам 394
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

LMTDEVSSN (ограничить сеансы одним
устройством), параметр
пользовательский профайл 98

LNKDTADFN (Подключить определение
данных), команда
контроля объекта 548
необходимые права доступа к
объектам 435

locale
права доступа к объектам,
необходимые для применения
команд 464

LOCALE (опции пользователя), параметр
пользовательский профайл 113

LODIMGCLG, команда
необходимые права доступа к
объектам 414

LODIMGCLGE, команда
необходимые права доступа к
объектам 414

LODOPTFMW
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

LODOPTFMW, команда
необходимые права доступа к
объектам 480

LODPTF (Загрузить временное
исправление программы), команда
необходимые права доступа к
объектам 504
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

LODQSTDV (Загрузить базу данных
вопросов и ответов), команда
необходимые права доступа к
объектам 495
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

LPR (Инициатор почтового принтера),
команда
необходимые права доступа к
объектам 516

M

MAXSTG (максимальный объем памяти),
параметр
владелец прав доступа
изменение на QDFTOWN (владелец
по умолчанию) 152
группа, принадлежность объектов 150
операция восстановления 99
получатель журнала 99
пользовательский профайл 99

MGRS36 (Выполнить миграцию
System/36), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36APF
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36CBL
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36DFU
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36DSPF
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36ITM (Выполнить миграцию
объекта System/36), команда
необходимые права доступа к
объектам 469
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36LIB
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36MNU
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36MSGF
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36QRY
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36RPG
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS36SEC
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MGRS38OBJ (Перенести объекты
System/38), команда
необходимые права доступа к
объектам 469
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

MIGRATE
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

ML (действия с почтой), тип записи
журнала 291

ML (действия с почтой), формат
файла 664

MOUNT (Добавить смонтированную
файловую систему), команда
необходимые права доступа к
объектам 472, 519

MOV
необходимые права доступа к
объектам 425

MOV (Переместить), команда
контроля объекта 541, 584, 585, 586,
587

MOVDOC (Переместить документ),
команда
контроля объекта 546
необходимые права доступа к
объектам 397

MOVOBJ (Переместить объект), команда
контроля объекта 528, 561
необходимые права доступа к
объектам 366

MRGDOC (Вставить документ), команда
контроля объекта 544, 546
необходимые права доступа к
объектам 398

MRGFORMD (Вставить описание формы),
команда
необходимые права доступа к
объектам 374

MRGMSGF (Вставить файл сообщений),
команда
контроля объекта 564, 565
необходимые права доступа к
объектам 468

MRGTCRPH (Вставить в таблицу хостов
TCP/IP), команда
объект, права доступа,
необходимые 517

MSGQ (очередь сообщений), параметр
пользовательский профайл 106

N

NA (изменение сетевых атрибутов), тип
записи журнала 298

NA (изменение сетевых атрибутов),
формат файла 665

ND (каталог APPN), формат файла 665

NE (конечная точка APPN), формат
файла 666

NETSTAT (Состояние сети), команда
необходимые права доступа к
объектам 517

NLV (национальный язык)
защита команд 248

O

OBJAUD (контроль за объектом),
параметр
пользовательский профайл 117

OM (управление объектом), тип записи
журнала 291

OPNDBF (Открыть файл базы данных),
команда
необходимые права доступа к
объектам 409

OPNQRYF (Открыть файл запроса),
команда
необходимые права доступа к
объектам 409

OPRCTL (управляется оператором),
параметр 223

OR (восстановление объекта), тип записи
журнала 293

OUTQ (очередь вывода), параметр
пользовательский профайл 108

OVRMSGF (Переопределить файл
сообщений), команда
контроля объекта 565

OW (изменение принадлежности), тип
записи журнала 298

OW (изменение принадлежности), формат
файла 675

OWNER (владелец), параметр
пользовательский профайл 152

P

PA (принятие прав доступа программой),
тип записи журнала 298

PA (принятие прав доступа программой),
формат файла 680

PAGDOC (Разбить документ на страницы),
команда
контроля объекта 546
необходимые права доступа к
объектам 398

PC (персональный компьютер)
запрет доступа 226

PC Organizer
отключение (системное значение
QINACTMSGQ) 30
разрешено для пользователя с
ограниченными возможностями 88

PCSACC (доступ к PC Support), сетевой
атрибут 277

PCSACC (обработка запросов клиентов),
сетевой атрибут 226

PG (изменение основной группы), тип
записи 298

PG (изменение основной группы), формат
файла 682

PING (Проверить соединение TCP/IP),
команда
объект, права доступа,
необходимые 517

PKGPRDDST (Упаковать рассылку
продукта), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

PO (вывод на принтер), тип записи 293

PO (вывод на принтер), формат
файла 685

printer
виртуальный
защита 227
пользовательский профайл 108

PRTACTRPT
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

PRTACTRPT (Печатать отчет об
операциях), команда
необходимые права доступа к
объектам 486

PRTADPOBJ (Печатать принимающие
объекты), команда
описание 754

PRTADPOBJ (Печать объекта с принятыми
правами доступа), команда
необходимые права доступа к
объектам 366

PRTCMDUSG (Печатать формат
команды), команда
контроля объекта 535, 572
необходимые права доступа к
объектам 492

PRTCMNSEC (Печатать параметры
защиты средств связи), команда
необходимые права доступа к
объектам 387

PRTCMNSEC (Печать параметров защиты
средств связи), команда
необходимые права доступа к
объектам 392, 463
описание 335, 754

PRTCMNTRC (Печатать данные
трассировки соединений), команда
необходимые права доступа к
объектам 504
пользовательские профайлы,
поставляемые IBM, с правами
доступа 353

PRTCPTRPT
пользовательские профайлы,
поставляемые IBM, с правами
доступа 354

PRTCPTRPT (Печатать отчет о
компонентах), команда
необходимые права доступа к
объектам 486

PRTCSPAPP (Печать приложения CSP/AE),
команда
контроля объекта 572

PRTDEVADR (Печатать адреса устройств),
команда
контроля объекта 538

PRTDEVADR (Печатать адреса устройств), команда *(продолжение)*
необходимые права доступа к объектам 384

PRTDOC (Печать документа), команда контроля объекта 544

PRTDSKINF
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTDSKINF (Печатать информацию о работе дисков), команда
необходимые права доступа к объектам 477

PRTERRLOG
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTERRLOG (Печатать протокол ошибок), команда
необходимые права доступа к объектам 504

PRTINTDTA
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTINTDTA (Печатать внутренние данные), команда
необходимые права доступа к объектам 504

PRTIPSCFG (Печатать конфигурацию IP для SNA), команда
необходимые права доступа к объектам 373

PRTJOBDAUT (Печать прав доступа к описаниям заданий), команда
необходимые права доступа к объектам 441
описание 334, 754

PRTJOBPRPT
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTJOBPRPT (Печатать отчет задания), команда
необходимые права доступа к объектам 486

PRTJOBTRC
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTJOBTRC (Печатать данные трассировки задания), команда
необходимые права доступа к объектам 486

PRTJVMJOB, команда
необходимые права доступа к объектам 437

PRTLCKRPT
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTLCKRPT (Печатать отчет о блокировках), команда
необходимые права доступа к объектам 486

PRTPEXRPT (Печатать отчет Индикатора статистики), команда
необходимые права доступа к объектам 487

PRTPOLRPT
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTPOLRPT (Печатать отчет о пулах), команда
необходимые права доступа к объектам 487

PRTPRFINT (Печать содержимого профайла), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTPUBAUT (Печатать общие права доступа), команда
необходимые права доступа к объектам 366

PRTPUBAUT (Печать объектов с общими правами доступа), команда
описание 334, 754

PRTPVTAUT (Печатать частные права доступа), команда
необходимые права доступа к объектам 366

PRTPVTAUT (Печать частных прав доступа), команда
описание 334, 756
список прав доступа 754

PRTQAUT (Печатать права доступа к очереди), команда
необходимые права доступа к объектам 442, 481

PRTQAUT (Печать прав доступа к очереди), команда
описание 334, 756

PRTRSRPT
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTRSRPT (Печатать отчет о ресурсах), команда
необходимые права доступа к объектам 487

PRTSBSDAUT (Печатать права доступа к описанию подсистемы), команда
необходимые права доступа к объектам 511
описание 334

PRTSBSDAUT (Печать описания подсистемы), команда
описание 754

PRTSQLINF (Печатать информацию языка структурных запросов), команда
необходимые права доступа к объектам 482

PRTSQLINF (Печать информации SQL), команда
контроль объекта 572, 583

PRTSYSRPT
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTSYSRPT (Печатать отчет о системе), команда
необходимые права доступа к объектам 487

PRTSYSSECA (Печать системных атрибутов защиты), команда
необходимые права доступа к объектам 502
описание 335, 754

PRTTNSRPT
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTTNSRPT (Печатать отчет о транзакциях), команда
необходимые права доступа к объектам 487

PRTTRC (Печатать данные трассировки), команда
необходимые права доступа к объектам 504

PRTTRCRPT
пользовательские профайлы, поставляемые IBM, с правами доступа 354

PRTTRGPGM (Печатать программу триггера), команда
необходимые права доступа к объектам 409

PRTTRGPGM (Печать программ триггеров), команда
описание 334, 754

PRTUSROBJ (Печатать пользовательские объекты), команда
необходимые права доступа к объектам 366

PRTUSROBJ (Печать пользовательских объектов), команда
описание 334, 754

PRTUSRPRF (Печать пользовательского профайла), команда
необходимые права доступа к объектам 521
описание 754

PS (смена профайла), тип записи журнала 299

PS (смена профайла), формат файла 687

PTF (временное исправление программы)
права доступа к объектам, необходимые для применения команд 502

PTYLMT (ограничение приоритета), параметр
пользовательский профайл 100
рекомендации 101

PW (пароль), тип записи журнала 287

PWDEXP (ограничить срок действия пароля), параметр 82

PWDEXPITV (срок действия пароля), параметр 96

PWRDWN SYS (Выключить систему), команда
необходимые права доступа к объектам 512
пользовательские профайлы, поставляемые IBM, с правами доступа 354

Q

- QADSM (ADSM), пользовательский профайл 339
- QAFDFTUSR (AFDFTUSR), пользовательский профайл 339
- QAFOWN (AFOWN), пользовательский профайл 339
- QAFUSR (AFUSR), пользовательский профайл 339
- QALWOBJRST (разрешить восстановление объектов), системное значение 48 значение, устанавливаемое командой CFGSYSSEC 759
- QALWUSRDMN (разрешить пользовательские объекты), системное значение 21, 27
- QASYADJE (изменение параметров контроля), формат файла 601
- QASYAFJE (отсутствие необходимых прав доступа), формат файла 604
- QASYARJE (принятые права доступа), формат файла 611
- QASYAUJ5 (изменение атрибутов), формат файла 611
- QASYCAJE (изменение прав доступа), формат файла 612
- QASYCDJE (командная строка), формат файла 615
- QASYCOJE (создание объекта), формат файла 616
- QASYCPJE (изменение пользовательского профайла), формат файла 618
- QASYCQJE (изменение *CRQD), формат файла 622
- QASYCUJ4 (операции с кластерами), формат файла 622
- QASYCVJ4 (проверка соединения), формат файла 624
- QASYCYJ4 (настройка шифрования), формат файла 626
- QASYCYJ4 (Сервер каталогов), формат файла 629
- QASYDOJE (операция удаления), формат файла 635
- QASYDSJE (сброс поставляемого IBM ИД пользователя сервисных средств), формат файла 637
- QASYEVJE (EV), формат файла 638
- QASYGRJ4 (шаблон записи), формат файла 639
- QASYGSJE (действия по обмену данными между процессами), формат файла 648
- QASYGSJE (предоставить дескриптор), формат файла 644
- QASYGSJE (управление защитой в Internet), формат файла 651
- QASYIRJ4 (действия правил обработки пакетов IP), формат файла 649
- QASYJDJE (изменение описания задания), формат файла 654
- QASYJSJE (изменение задания), формат файла 655
- QASYKFJ4 (файл набора ключей), формат файла 659
- QASYLDJE (создание и удаление связей, поиск в каталоге), формат файла 663
- QASYMLJE (действия с почтой), формат файла 664
- QASYNAJE (изменение сетевых атрибутов), формат файла 665
- QASYNDJE (каталог APPN), формат файла 665
- QASYNEJE (конечная точка APPN), формат файла 666
- QASYOIJE (доступ к оптической памяти), формат файла 677, 678
- QASYOZJE (доступ к оптической памяти), формат файла 679
- QASYOMJE (управление объектами), формат файла 667
- QASYORJE (восстановление объекта), формат файла 671
- QASYOWJE (изменение принадлежности), формат файла 675
- QASYPAJE (принятие прав доступа программой), формат 680
- QASYPGJE (изменение основной группы), формат 682
- QASYPOJE (вывод на принтер), формат файла 685
- QASYPSJE (смена профайла), формат 687
- QASYPWJE (пароль), формат 689
- QASYRAJE (изменение прав доступа восстановленного объекта), формат файла 690
- QASYRJE (восстановление описания задания), формат файла 692
- QASYROJE (изменение владельца объектной программы), формат файла 693
- QASYRPJE (восстановление программ, принимающих права доступа), формат файла 695
- QASYRQJE (восстановление объекта *CRQD, принимающего права доступа), формат файла 697
- QASYRUJE (восстановить права доступа пользовательского профайла), формат файла 698
- QASYRZJE (изменение основной группы восстановленного объекта), формат файла 698
- QASYSDJE (изменить системный каталог рассылки), формат файла 700
- QASYSEJE (изменение записи о выполнении подсистемы), формат файла 702
- QASYSFJE (действие над буферным файлом), формат файла 703
- QASYSGJ4(), формат файла 707, 709
- QASYSMJE (изменение параметров управления системами), формат файла 710
- QASYSOJ4 (действия над пользовательской информацией о защите сервера), формат файла 711
- QASYSTJE (обращение к сервисным средствам), формат файла 712
- QASYSVJE (действие над системным значением), формат файла 718
- QASYVAJE (изменение списка управления доступом), формат файла 719
- QASYVCJE (запуск и завершение соединения), формат файла 720
- QASYVFJE (закрытие файлов сервера), формат файла 721
- QASYVLJE (превышено ограничение для учетной записи), формат файла 721
- QASYVNJE (вход в сеть и выход из нее), формат файла 722
- QASYVOJ4 (контрольный список), формат файла 723
- QASYVPJE (ошибка в сетевом пароле), формат файла 725
- QASYVRJE (обращение к сетевому ресурсу), формат файла 726
- QASYVSJE (сеанс сервера), формат файла 727
- QASYVUJE (изменение сетевого профайла), формат файла 728
- QASYVVJE (изменилось состояние службы), формат файла 729
- QASYX0JE (идентификация Kerberos), формат файла 730
- QASYXCJE (изменение объекта DLO), формат файла 738
- QASYYRJE (чтение объекта DLO), формат файла 739
- QASYZCJE (изменение объекта), формат файла 740
- QASYZRJE (чтение объекта), формат файла 743
- QATNPGM (программа обработки клавиши Attention), системное значение 110
- QAUDCTL (управление контролем), системное значение изменение 334, 751 обзор 69 просмотр 334, 751
- QAUDENDACN (действие при сбое контроля), системное значение 69, 307
- QAUDFRCLVL (уровень выгрузки записей контроля), системное значение 70, 306
- QAUDJRN (контроль), журнал 298, 302, 527
- AD (изменение контроля), тип записи 297
- AD (изменение параметров контроля), формат файла 601
- AF (отсутствие необходимых прав доступа), формат файла 604
- AF (ошибка прав доступа), тип записи 292
- запрещенная команда 19
- нарушение аппаратной защиты 18
- нарушение входа в систему по умолчанию 17
- нарушение описания задания 17
- неподдерживаемый интерфейс 17, 19
- описание 286
- проверка программы 19
- AP (принятые права доступа), тип записи 292
- AP (принятые права доступа), формат файла 611
- AU (изменение атрибутов), формат файла 611

QAUDJRN (контроль), журнал
(продолжение)

CA (изменение прав доступа), тип записи 297
CA (изменение прав доступа), формат файла 612
CD (командная строка), формат файла 615
CD (текст команды), тип записи 288
CO (создание объекта), тип записи 151, 288
CO (создание объекта), формат файла 616
CP (изменение пользовательского профайла), тип записи 294
CP (изменение пользовательского профайла), формат файла 618
CQ (изменение *CRQD), формат файла 622
CQ (изменение объекта *CRQD), тип записи 294
CU (операции с кластерами), формат файла 622
CV (проверка соединения), формат файла 624
CY (настройка шифрования), формат файла 626
DI (Сервер каталогов), формат файла 629
DO (операция удаления), тип записи 288
DO (операция удаления), формат файла 635
DS (сброс пароля DST), тип записи 294
DS (сброс поставляемого IBM ИД пользователя сервисных средств), формат файла 637
EV (переменная среды), формат файла 638
GR (шаблон записи), формат файла 639
GS (предоставить дескриптор), формат файла 644
IP (действия по обмену данными между процессами), формат файла 648
IP (межпроцессорная связь), тип записи 287
IR (действия правил обработки пакетов IP), формат файла 649
IS (управление защитой в Internet), формат файла 651
JD (изменение описания задания), тип записи 298
JD (изменение описания задания), формат файла 654
JS (изменение задания), тип записи 289
JS (изменение задания), формат файла 655
KF (файл набора ключей), формат файла 659
LD (создание и удаление связей, поиск в каталоге), формат файла 663
ML (действия с почтой), тип записи 291

QAUDJRN (контроль), журнал
(продолжение)

ML (действия с почтой), формат файла 664
NA (изменение сетевых атрибутов), тип записи 298
NA (изменение сетевых атрибутов), формат файла 665
ND (каталог APPN), формат файла 665
NE (конечная точка APPN), формат файла 666
O1 (доступ к оптической памяти), формат файла 677, 678
O3 (доступ к оптической памяти), формат файла 679
OM (управление объектами), формат файла 667
OM (управление объектом), тип записи 291
OR (восстановление объекта), тип записи 293
OR (восстановление объекта), формат файла 671
OW (изменение принадлежности), тип записи 298
OW (изменение принадлежности), формат файла 675
PA (принятие прав доступа программой), тип записи 298
PA (принятие прав доступа программой), формат файла 680
PG (изменение основной группы), тип записи 298
PG (изменение основной группы), формат файла 682
PO (вывод на принтер), тип записи 293
PO (вывод на принтер), формат файла 685
PS (смена профайла), тип записи 299
PS (смена профайла), формат файла 687
PW (пароль), тип записи 287
PW (пароль), формат файла 689
RA (изменение прав доступа восстановленного объекта), формат файла 690
RA (изменение прав доступа к восстановленным объектам), тип записи 293
RJ (восстановление описания задания), тип записи 293
RJ (восстановление описания задания), формат файла 692
RO (изменение владельца восстановленного объекта), формат файла 693
RO (изменение принадлежности восстановленного объекта), тип записи 293
RP (восстановление программ, принимающих права доступа), тип записи 293
RP (восстановление программ, принимающих права доступа), формат файла 695

QAUDJRN (контроль), журнал
(продолжение)

RQ (восстановление объекта *CRQD), тип записи 293
RQ (восстановление объекта *CRQD, принимающего права доступа), формат файла 697
RU (восстановить права доступа пользовательского профайла), формат файла 698
RU (восстановление прав доступа пользовательского профайла), тип записи 293
RZ (изменение основной группы восстановленного объекта), тип записи 293
RZ (изменение основной группы восстановленного объекта), формат файла 698
SD (изменение системного каталога рассылки), тип записи 291
SD (изменить системный каталог рассылки), формат файла 700
SE (изменение записи маршрутизации подсистемы), тип записи 299
SE (изменение записи о выполнении подсистемы), формат файла 702
SF (действие над буферным файлом), формат файла 703
SF (изменение буферного файла), тип записи 301
SG, формат файла 707, 709
SM (изменение параметров управления системами), формат файла 710
SM (изменение управления системами), тип записи 302
SO (действия над пользовательской информацией о защите сервера), формат файла 711
ST (действия сервисных средств), тип записи 301
ST (обращение к сервисным средствам), формат файла 712
SV (действие над системным значением), формат файла 718
SV (действия с системными значениями), тип записи 299
VA (изменение списка управления доступом), тип записи 299
VA (изменение списка управления доступом), формат файла 719
VC (запуск и завершение соединения), формат файла 720
VC (начало или завершение соединения), тип записи 289
VF (заккрытие файлов сервера), формат файла 721
VL (превышено ограничение для учетной записи), формат файла 721
VN (вход в сеть и выход из нее), формат файла 722
VN (вход или выход из сети), тип записи 289
VO (контрольный список), формат файла 723
VP (ошибка в сетевом пароле), формат файла 725

- QAUDJRN (контроль), журнал
(*продолжение*)
- VP (ошибка сетевого пароля), тип записи 288
 - VR (обращение к сетевому ресурсу), формат файла 726
 - VS (сеанс сервера), тип записи 289
 - VS (сеанс сервера), формат файла 727
 - VU (изменение сетевого профайла), формат файла 728
 - VU(изменение сетевого профайла), тип записи 299
 - VV (изменение состояния обслуживания), тип записи 301
 - VV (изменилось состояние службы), формат файла 729
 - X0 (идентификация Kerberos), формат файла 730
 - YC (изменение объекта DLO), формат файла 738
 - YR (чтение объекта DLO), формат файла 739
 - ZC (изменение объекта), формат файла 740
 - ZR (чтение объекта), формат файла 743
 - автоматическая очистка 311
 - анализ
 - с помощью запроса 315
 - введение 277
 - завершение 313
 - замена получателя 312
 - отключение получателя 311, 312
 - ошибки 69
 - поврежденный 310
 - порог памяти получателя 310
 - просмотр записей 278, 313
 - расширение уровня контроля (QAUDLVL2), системное значение 72
 - системные записи 310
 - создание 309
 - способы анализа 313
 - управление 310
 - уровень контроля (QAUDLVL), системное значение 71
 - уровень сохранения 70
- QAUDLVL (уровень контроля), системное значение
- *AUTFAIL, значение 286
 - *CREATE (создание), значение 288
 - *DELETE (удаление), значение 288
 - *JOBDDTA (изменение задания), значение 289
 - *OBJMGT (управление объектом), значение 291
 - *OFCSRV (функции Office), значение 291
 - *PGMADP(принятые права доступа), значение 292
 - *PGMFAIL (сбой программы), значение 292
 - *PRTDDTA (вывод на принтер), значение 293
 - *SAVRST (сохранение/восстановление), значение 293
 - *SECURITY (защита), значение 297
- QAUDLVL (уровень контроля), системное значение (*продолжение*)
- *SERVICE (сервисные средства), значение 301
 - *SPLFDDTA (изменения буферного файла), значение 301
 - *SYSMGT (управление системами), значение 301
 - изменение 309, 334, 751
 - обзор 71
 - пользовательский профайл 118
 - просмотр 334, 751
 - цель 278
- QAUDLVL2 (расширение уровня контроля), системное значение
- обзор 72
- QAUTOFCFG (автоматическая настройка устройств), системное значение 40
- QAUTOFCFG (автоматическая настройка), системное значение
- значение, устанавливаемое командой CFGSYSSECC 759
- QAUTOVRT (автоматическая настройка виртуальных устройств), системное значение 41
- значение, устанавливаемое командой CFGSYSSECC 759
- QAUTPROF (профайл прав доступа) 339
- QBRMS (BRM), пользовательский профайл 339
- QCCSID (идентификатор набора символов), системное значение 112
- QCL, программа 144
- QCNTYID (идентификатор страны или региона), системное значение 111
- QCONSOLE (консоль), системное значение 213
- QCRTAUT (права при создании), системное значение
- использование 146
 - описание 28
 - риск изменения 28
- QCRTOBJAUD (создать контроль за объектом), системное значение 74
- QDBSHRDO (общая база данных), пользовательский профайл 339
- QDCEADM (DCEADM), пользовательский профайл 339
- QDEVRACYACN (действие для восстановления устройства), системное значение 41
- значение, устанавливаемое командой CFGSYSSECC 759
- QDFTJOBDD (по умолчанию), описание задания 101
- QDFTOWN (владелец по умолчанию), пользовательский профайл
- восстановление программ 267
 - запись журнала контроля (QAUDJRN) 293
 - значения по умолчанию 339
 - описание 152
- QDOC (документ), пользовательский профайл 339
- QDSCJOBITV (тайм-аут отключенного задания), системное значение 42
- QDSCJOBITV (тайм-аут отключенного задания), системное значение (*продолжение*)
- значение, устанавливаемое командой CFGSYSSECC 759
- QDSNX (узловой исполнитель в распределенных системах), пользовательский профайл 339
- QDSPSGNINF (показать информацию о входе в систему), системное значение 29, 96
- значение, устанавливаемое командой CFGSYSSECC 759
- QEZMAIN, программа 110
- QFNC (финансы), пользовательский профайл 339
- QGATE (мост VM/MVS), пользовательский профайл 339
- QHST (протокол хронологии) применение для контроля за защитой 318
- QINACTITV (тайм-аут неактивного задания), системное значение 29
- значение, устанавливаемое командой CFGSYSSECC 759
- QINACTMSGQ (очередь сообщений неактивного задания), системное значение 30
- значение, устанавливаемое командой CFGSYSSECC 759
- QjoAddRemoteJournal (Добавить удаленный журнал), API
- контроль объекта 559
- QjoChangeJournal (Изменить состояние журнала), API
- контроль объекта 559
- QjoEndJournal (Завершить ведение журнала), API
- контроль объекта 528, 559
- QJORDJE2, формат записи 594
- QjoRemoveRemoteJournal (Удалить удаленный журнал), API
- контроль объекта 559
- QjoRetrieveJournalEntries (Получить записи журнала), API
- контроль объекта 559
- QjoRetrieveJournalInformation (Получить информацию о журнале), API
- контроль объекта 560
- QJORJIDI (Получить информацию об идентификаторе журнала (JID)), API
- контроль объекта 559
- QjoSJRNE (Отправить запись журнала), API
- контроль объекта 560
- QjoStartJournal (Начать ведение журнала), API
- контроль объекта 528, 560
- QKBDDBUF (буферизация клавиатуры), системное значение 99
- QLANGID (идентификатор языка), системное значение 111
- QlgAccess, команда (Определить доступные файлы)
- контроль объекта 540

- QlgAccessx, команда (Определить доступные файлы)
контроля объекта 540
- QLMTDEVSSN (ограничить сеансы одним устройством), системное значение
LMTDEVSSN пользовательский профайл, параметр 98
описание 31
параметров контроля 274
- QLMTSECOFR (ограничить права системного администратора), системное значение
вход в систему 213
значение, устанавливаемое командой CFGSYSSEC 759
изменение уровня защиты 14
описание 32
параметров контроля 272
права доступа к описаниям устройств 211
- QLPAUTO (пользовательский профайл автоматической установки лицензионных программ)
восстановление 263
значения по умолчанию 339
- QLPINSTALL (установка лицензионных программ), пользовательский профайл
восстановление 263
значения по умолчанию 339
- QMAXSGNACN (действие при достижении максимального числа попыток входа в систему), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
описание 33
состояние пользовательского профайла 83
- QMAXSIGN (максимальное число попыток входа в систему), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
описание 32
параметров контроля 272, 276
состояние пользовательского профайла 83
- QMSF (среда почтового сервера), пользовательский профайл 339
- QPGMR (профайл программиста)
значения по умолчанию 339
описание устройства, владелец 213
пароль, устанавливаемый командой CFGSYSSEC 761
- QPRTDEV (принтер), системное значение 108
- QPWDCHGBLK (блокировка изменения пароля), системное значение
описание 51
- QPWDEXPITV (срок действия пароля), системное значение
PWDEXPITV пользовательский профайл, параметр 96
значение, устанавливаемое командой CFGSYSSEC 759
описание 51
параметров контроля 273
- QPWDEXPWRN (предупреждение об истечении срока действия пароля), системное значение
описание 52
- QPWDLMTAJC (запрет цифр в соседних позициях в пароле), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
- QPWDLMTAJC (запретить применение последовательности цифр), системное значение 55
- QPWDLMTCHR (запретить некоторые символы), системное значение 55
- QPWDLMTCHR (недопустимые для пароля символы), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
- QPWDLMTREP (запрет повторяющихся символов в пароле), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
- QPWDLMTREP (запретить повторяющиеся символы), системное значение 56
- QPWDLVL
Уровни паролей (QPWDLVL) 53, 54, 55
уровни паролей (максимальная длина) 54
уровни паролей (минимальная длина) 53
учет регистра символов в пароле 57, 80
- QPWDLVL (с учетом регистра)
Уровни паролей (с учетом регистра) 56
учет регистра символов в пароле QPWDLVL с учетом регистра символов 56
- QPWDLVL (текущее или ожидающее значение) и имя программы 63
- QPWDMAXLEN (максимальная длина пароля), системное значение 54
значение, устанавливаемое командой CFGSYSSEC 759
- QPWDMINLEN (минимальная длина пароля), системное значение 53
значение, устанавливаемое командой CFGSYSSEC 759
- QPWDPOSDIF (символы в одинаковых позициях), системное значение 57
- QPWDRQDDGT (обязательное вхождение в пароль цифр), системное значение 57
- QPWDRQDDGT (требовать наличия цифр в пароле), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
- QPWDRQDDIF (обязательное изменение пароля), системное значение 54
- QPWDRQDDIF (проверка совпадения паролей), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
- QPWDVLDPGM (программа проверки пароля), системное значение 63
значение, устанавливаемое командой CFGSYSSEC 759
- QRCL (восстановить память), библиотека
QALWUSRDMN (разрешить пользовательские объекты), системное значение 28
- QRCLAUTL (восстановление памяти), список прав доступа 269
- QRETSVRSEC (сохранить идентификационные данные на сервере), значение 34
- QRETSVRSEC (сохранить идентификационные данные на сервере), системное значение 34
- QRJE (запись удаленного задания), пользовательский профайл 339
- QRMTSIGN (разрешить удаленный вход в систему), системное значение
значение, устанавливаемое командой CFGSYSSEC 759
- QRMTSIGN (удаленный вход в систему), системное значение 35, 277
- QRMTSRVATR (атрибут удаленного обслуживания), системное значение 2, 42
- QRYDOCLIB (Запросить библиотеку документов), команда
контроля объекта 546
необходимые права доступа к объектам 398
- QRYDST (Запросить рассылку), команда
необходимые права доступа к объектам 395
- QRYPRBSTS (Запросить состояние неполадки), команда
необходимые права доступа к объектам 489
- QSCANFS (Сканирование в файловых системах), системное значение 36
- QSCANFCTL (Управление сканированием в файловых системах), системное значение 36
- QSECOFR (пользовательский профайл системного администратора)
восстановление 263
значения по умолчанию 339
описание устройства, владелец 213
отключен, состояние 83
права доступа к консоли 213
разрешение применения 83
- QSECURITY (уровень защиты), системное значение
автоматическое создание пользовательских профайлов 77
введение 2
внутренние управляющие блоки 22
значение, устанавливаемое командой CFGSYSSEC 759
класс пользователя 11
обзор 9
отключение уровня 40 20
отключение уровня 50 22
параметров контроля 272
переход на уровень 40 19
переход, на уровень 20 с более высокого 13
переход, на уровень 50 22
переход, с уровня 10 на уровень 20 13
переход, с уровня 20 на уровень 30 13

QSECURITY (уровень защиты), системное значение (*продолжение*)
 применение системного значения QLMTSECOFR 213
 рекомендации 11
 специальные права доступа 11
 сравнение уровней 9
 уровень 10 12
 уровень 20 12
 уровень 30 13
 уровень 40 14
 уровень 50 20
 обработка сообщений 21
 проверка параметров 18
 QSH (Запустить QSH), команда псевдоним для STRQSH 493
 QSHRMEMCTL (управление общей памятью), системное значение возможные значения 38
 описание 38
 QSNADS (службы рассылки системной сетевой архитектуры), пользовательский профайл 339
 QSPCENV (специальная среда), системное значение 94
 QSPL (буфер), пользовательский профайл 339
 QSPLJOB (буферное задание), пользовательский профайл 339
 QSPRJOBQ (Получить информацию об очереди заданий), API контроля объекта 558
 QsrRestore
 контроля объекта 529
 QSRRSTO (Восстановить объект), API контроля объекта 528
 QsrSave
 контроля объекта 527
 QSRSAVO
 контроля объекта 527
 QSRTSEQ (последовательность сортировки), системное значение 110
 QSRV (служебный пользовательский профайл)
 значения по умолчанию 339
 пароль, устанавливаемый командой CFGSYSSEC 761
 права доступа к консоли 213
 QSRVBAS (основной служебный пользовательский профайл)
 значения по умолчанию 339
 пароль, устанавливаемый командой CFGSYSSEC 761
 права доступа к консоли 213
 QSSLSL (список шифров SSL), системное значение 43
 QSSLSLCTL (управление шифрами SSL), системное значение 44
 QSSLPCL (протоколы SSL), системное значение 44
 QSYS (системный пользовательский профайл)
 восстановление 263
 значения по умолчанию 339
 QSYS, системная библиотека списков прав доступа 145

QSYSLIBL (список системных библиотек), системное значение 218
 QSYSOPR (очередь сообщений системного оператора)
 ограничение 217
 QSYSOPR (профайл системного оператора) 339
 пароль, устанавливаемый командой CFGSYSSEC 761
 QTCP (TCP/IP), пользовательский профайл 339
 QTEMP (временная), библиотека уровень защиты 50 21
 QTMLPD (поддержка печати по TCP/IP), пользовательский профайл 339
 QTSTRQS (тестовый запрос), пользовательский профайл 339
 Query Management/400
 права доступа к объектам, необходимые для применения команд 494
 QUSEADPAUT (Применять принятые права доступа), системное значение описание 38
 риск изменения 39
 QUSER (пользователь рабочей станции), пользовательский профайл 339
 QUSER (профайл пользователя)
 пароль, устанавливаемый командой CFGSYSSEC 761
 QUSER38, библиотека 144
 QVfyOvBJRST (Проверять восстанавливаемые объекты) системное значение 3
 QWCLSCDE (Показать запись расписания заданий), API контроля объекта 559

R

RA (изменение прав доступа к восстановленным объектам), тип записи журнала 293
 RCLACTGRP (Восстановить группу активации), команда
 необходимые права доступа к объектам 512
 RCLDBXREF, команда
 необходимые права доступа к объектам 366
 пользовательские профайлы, поставляемые IBM, с правами доступа 354
 RCLDLO (Восстановить объект библиотеки документов), команда контроля объекта 547
 необходимые права доступа к объектам 398
 RCLLNK (Восстановить ссылки объекта), команда
 необходимые права доступа к объектам 426
 RCLOBJOWN (Восстановить объекты по владельцу), команда
 необходимые права доступа к объектам 366
 RCLOBJOWN (Восстановить объекты по владельцу), команда (*продолжение*)
 пользовательские профайлы, поставляемые IBM, с правами доступа 354
 RCLOPT (Восстановить оптический носитель), команда
 необходимые права доступа к объектам 480
 пользовательские профайлы, поставляемые IBM, с правами доступа 354
 RCLRSC (Восстановить ресурсы), команда объект необходимые права доступа 512
 RCLSPLSTG (Восстановить буферную память), команда
 необходимые права доступа к объектам 509
 пользовательские профайлы, поставляемые IBM, с правами доступа 354
 RCLSTG (Восстановить память), команда QALWUSRDMN (разрешить пользовательские объекты), системное значение 28
 QDFTOWN (владелец по умолчанию), профайл 152
 контроля объекта 529
 необходимые права доступа к объектам 366
 поврежденный список прав доступа 269
 пользовательские профайлы, поставляемые IBM, с правами доступа 354
 уровень защиты 50 21
 RCLTMPSTG (Восстановить временную память), команда
 контроля объекта 530
 необходимые права доступа к объектам 366
 пользовательские профайлы, поставляемые IBM, с правами доступа 354
 RCV DST (Получить рассылку), команда
 контроля объекта 546
 необходимые права доступа к объектам 396
 RCVJRNE (Принять запись журнала), команда
 контроля объекта 559
 необходимые права доступа к объектам 446
 RCV MGRDTA (Принять переносимые данные), команда
 необходимые права доступа к объектам 468
 RCVMSG (Принять сообщение), команда
 контроля объекта 565, 566
 необходимые права доступа к объектам 467
 RCVNETF (Принять сетевой файл), команда
 необходимые права доступа к объектам 471

RESMGRNAM (Обработать повторные и неверные имена объектов Office), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RETURN (Возврат), команда
необходимые права доступа к объектам 512

RGZDLO (Реорганизовать объект библиотеки документов), команда
контроля объекта 546
необходимые права доступа к объектам 398

RGZPFM (Реорганизовать элемент физического файла), команда
контроля объекта 552
необходимые права доступа к объектам 410

RJ (восстановление описания задания), тип записи журнала 293

RJ (восстановление описания задания), формат файла 692

RJE (запись удаленного задания) права доступа к объектам, необходимые для применения команд 498

RLSCMNDEV (Разблокировать устройство связи), команда
контроля объекта 539, 562
необходимые права доступа к объектам 392
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RLSDSTQ (Разблокировать очередь рассылки), команда
необходимые права доступа к объектам 396
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RLSIFSLCK (Освободить блокировки IFS), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RLSIFSLCK (Удалить блокировку IFS), команда
необходимые права доступа к объектам 472

RLSJOB (Разблокировать задание), команда
необходимые права доступа к объектам 438

RLSJOBQ (Разблокировать очередь заданий), команда
контроля объекта 557
необходимые права доступа к объектам 442

RLSJOBSUDE (Разблокировать запись расписания заданий), команда
контроля объекта 558
необходимые права доступа к объектам 443

RLSOUTQ (Разблокировать очередь вывода), команда
контроля объекта 569
необходимые права доступа к объектам 481

RLSRDR (Разблокировать программу чтения), команда
необходимые права доступа к объектам 496

RLSRMTPHS (Освободить удаленную фазу), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RLSSPLF (Разблокировать буферный файл), команда
контроля объекта 569
необходимые права доступа к объектам 509

RLSWTR (Разблокировать загрузчик), команда
необходимые права доступа к объектам 524

RMVACC (Удалить код доступа), команда
контроля объекта 546
необходимые права доступа к объектам 476
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVAJE (Удалить запись автоматического задания), команда
контроля объекта 577
необходимые права доступа к объектам 511

RMVALRD (Удалить описание предупреждения), команда
контроля объекта 531
необходимые права доступа к объектам 373

RMVAUTLE (Удалить запись списка прав доступа), команда
использование 175
контроля объекта 531
необходимые права доступа к объектам 376
описание 327

RMVBKP (Удалить точку прерывания), команда
необходимые права доступа к объектам 492

RMVBNDDIRE (Удалить запись каталога связывания), команда
контроля объекта 532
необходимые права доступа к объектам 376

RMVCFGLE (Удалить записи списка конфигурации), команда
необходимые права доступа к объектам 385

RMVCFGLE (Удалить запись списка конфигурации), команда
контроля объекта 533

RMVCLUNODE
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVCLUNODE, команда
необходимые права доступа к объектам 381

RMVCMNE (Удалить запись средств связи), команда
контроля объекта 577
необходимые права доступа к объектам 511

RMVCNNLE (Удалить запись списка соединений), команда
контроля объекта 536

RMVCOMSNMP (Удалить взаимодействие для SNMP), команда
необходимые права доступа к объектам 517

RMVCRGDEVE
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVCRGNODE
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVCRQD (Удалить операцию из описания запроса на изменение), команда
контроля объекта 535

RMVCRQDA (Удалить операцию описания запроса на изменение), команда
необходимые права доступа к объектам 377

RMVCRSDMKN (Удалить междоменный ключ шифрования ключа), команда
необходимые права доступа к объектам 389
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVDEVDMNE, команда
необходимые права доступа к объектам 382
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVDFRID (Удалить отложенный ИД), команда
контроля объекта 530

RMVDFRID, команда
пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVDIR (Удалить каталог), команда
контроля объекта 541
необходимые права доступа к объектам 426

RMVDIRE (Удалить запись каталога), команда
необходимые права доступа к объектам 393
описание 333

RMVDIRSHD (Удалить теневой каталог), команда
необходимые права доступа к объектам 393

RMVDLOAUT (Удалить права доступа к объекту библиотеки документов), команда
контроля объекта 546

RMVDLOAUT (Удалить права доступа к объекту библиотеки документов), команда *(продолжение)* необходимые права доступа к объектам 398 описание 332

RMVDSTLE (Удалить запись списка рассылки), команда необходимые права доступа к объектам 396

RMVDSTQ (Удалить очередь рассылки), команда необходимые права доступа к объектам 396 пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVDSTRTE (Удалить маршрут рассылки), команда необходимые права доступа к объектам 396 пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVDSTSYSN (Удалить альтернативное имя системы для рассылки), команда необходимые права доступа к объектам 396 пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVDWDFN, команда 354

RMVEMLCFGE (Удалить запись конфигурации эмуляции), команда необходимые права доступа к объектам 393

RMVENVVAR (Удалить переменную среды), команда необходимые права доступа к объектам 403

RMVEWCBCDE (Удалить запись штрихового кода для контроллера расширенной беспроводной сети), команда необходимые права доступа к объектам 404

RMVEWCPTCE (Удалить запись PTC контроллера расширенной беспроводной сети), команда необходимые права доступа к объектам 404

RMVEXITPGM (Удалить программу выхода), команда контроля объекта 550 необходимые права доступа к объектам 496 пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVFCSTE (Удалить запись таблицы управления формами), команда необходимые права доступа к объектам 500

RMVFNTTBLE (Удалить запись таблицы шрифтов DBCS) права доступа к объектам, необходимые для применения команд 373

RMVFTRACNE (Удалить запись о действии фильтра), команда контроля объекта 555 необходимые права доступа к объектам 412

RMVFTRSLTE (Удалить запись о выборе фильтра), команда контроля объекта 555 необходимые права доступа к объектам 412

RMVICFDEVE (Удалить запись об устройстве функции межсистемной связи), команда необходимые права доступа к объектам 410

RMVIMGCLGE, команда необходимые права доступа к объектам 414

RMVIPSFIC (Удалить интерфейс IP для SNA), команда необходимые права доступа к объектам 373

RMVIPSLC (Удалить запись о расположении IP для SNA), команда необходимые права доступа к объектам 373

RMVIPSRTE (Удалить маршрут IP для SNA), команда необходимые права доступа к объектам 373

RMVJOBQE (Удалить запись очереди заданий), команда контроля объекта 558, 577 необходимые права доступа к объектам 511

RMVJOBSCDE (Удалить запись расписания заданий), команда контроля объекта 558 необходимые права доступа к объектам 443

RMVJRNCHG (Удалить зарегистрированные изменения), команда контроля объекта 529, 560 необходимые права доступа к объектам 446 пользовательские профайлы, поставляемые IBM, с правами доступа 354

RMVJWDFN, команда 354

RMVLANADP (Удалить адаптер LAN), команда пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVLANADPT (Удалить адаптер LAN), команда необходимые права доступа к объектам 464

RMVLIBLE (Удалить запись списка библиотек), команда использование 218

RMVLICKEY (Удалить ключ лицензии), команда необходимые права доступа к объектам 461

RMVLNPK (Удалить ссылку), команда контроля объекта 580, 585, 587 необходимые права доступа к объектам 427

RMVM (Удалить элемент), команда контроля объекта 553 необходимые права доступа к объектам 410

RMVMFS (Удалить смонтированную файловую систему) необходимые права доступа к объектам 519

RMVMFS (Удалить смонтированную файловую систему), команда необходимые права доступа к объектам 472 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVMSG (Удалить сообщение), команда контроля объекта 566 необходимые права доступа к объектам 467

RMVMSGD (Удалить описание сообщения), команда контроля объекта 565 необходимые права доступа к объектам 467

RMVNETJOBE (Удалить запись сетевого задания), команда необходимые права доступа к объектам 471 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVNETTBLE (Удалить запись таблицы сетей), команда необходимые права доступа к объектам 517

RMVNODLE (Удалить запись списка узлов), команда контроля объекта 567 необходимые права доступа к объектам 476

RMVNWSSTGL (Отключить область памяти сетевого сервера), команда необходимые права доступа к объектам 474

RMVOPTCTG (Удалить оптическую кассету), команда необходимые права доступа к объектам 480 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVOPTSVR (Удалить оптический сервер), команда
 необходимые права доступа к объектам 480
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVPEXDFN (Удалить определение PEX), команда
 необходимые права доступа к объектам 487
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVPEXFTR (Удалить фильтр PEX), команда
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVPCST (Удалить ограничение для физического файла), команда
 контроля объекта 553
 необходимые права доступа к объектам 410

RMVPFTGR (Удалить триггер для физического файла), команда
 контроля объекта 553

RMVPFTRG (Удалить триггер для физического файла), команда
 необходимые права доступа к объектам 410

RMVPGM (Удалить программу), команда
 необходимые права доступа к объектам 492

RMVPE (Удалить запись предварительного задания), команда
 контроля объекта 578
 необходимые права доступа к объектам 511

RMVPTF (Удалить временное исправление программы), команда
 необходимые права доступа к объектам 504
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVRDBDIRE (Удалить запись каталога реляционной базы данных), команда
 необходимые права доступа к объектам 497

RMVRJECMNE (Удалить запись средств связи RJE), команда
 необходимые права доступа к объектам 501

RMVRJERDRE (Удалить запись программы чтения RJE), команда
 необходимые права доступа к объектам 501

RMVRJEWTR (Удалить запись программы записи RJE), команда
 необходимые права доступа к объектам 501

RMVRMTJRN (Удалить удаленный журнал), команда
 контроля объекта 560

RMVRMPTPF (Удалить удаленное временное исправление программы), команда
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVRPYLE (Удалить запись списка ответов), команда
 контроля объекта 576
 необходимые права доступа к объектам 513
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVRTGE (Удалить запись о выполнении), команда
 контроля объекта 578
 необходимые права доступа к объектам 511

RMVVSCHIDX (Удалить запись индекса поиска), команда
 контроля объекта 578
 необходимые права доступа к объектам 436

RMVSOCE (Удалить запись сферы управления), команда
 необходимые права доступа к объектам 508

RMVSVRAUTE (Удалить запись идентификации сервера), команда
 необходимые права доступа к объектам 502

RMVTAPCTG (Удалить кассету магнитной ленты), команда
 необходимые права доступа к объектам 465

RMVTCRHTE (Удалить запись таблицы хостов TCP/IP), команда
 необходимые права доступа к объектам 517

RMVTCRIFC (Удалить интерфейс TCP/IP), команда
 необходимые права доступа к объектам 517

RMVTCRPORT (Удалить ограничение на порт TCP/IP), команда
 необходимые права доступа к объектам 517

RMVTCRPSI (Удалить удаленную систему TCP/IP), команда
 необходимые права доступа к объектам 517

RMVTCRPRTE (Удалить маршрут TCP/IP), команда
 необходимые права доступа к объектам 517

RMVTRC (Удалить трассировку), команда
 необходимые права доступа к объектам 492

RMVTRCFTR
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

RMVWSE (Удалить запись рабочей станции), команда
 контроля объекта 578
 необходимые права доступа к объектам 511

RNM (Переименовать), команда
 контроля объекта 541, 580, 585, 587
 необходимые права доступа к объектам 427

RNMCNNLE (Переименовать запись списка соединений), команда
 контроля объекта 536

RNMDIRE (Переименовать запись каталога), команда
 необходимые права доступа к объектам 393

RNMDKT (Изменить имя дискеты), команда
 необходимые права доступа к объектам 465

RNMDLO (Переименовать объект библиотеки документов), команда
 контроля объекта 546
 необходимые права доступа к объектам 398

RNMDSTL (Переименовать список рассылки), команда
 необходимые права доступа к объектам 396

RNMM (Переименовать элемент), команда
 контроля объекта 553
 необходимые права доступа к объектам 410

RNMOBJ (Переименовать объект), команда
 контроля объекта 529, 561, 587
 необходимые права доступа к объектам 366

RNMTCRHTE (Переименовать запись таблицы хоста TCP/IP), команда
 необходимые права доступа к объектам 517

RO (изменение владельца восстановленного объекта), формат файла 693

RO (изменение принадлежности восстановленного объекта), тип записи журнала 293

ROLLBACK (Откат), команда
 необходимые права доступа к объектам 383

RP (восстановление программ, принимающих права доступа), тип записи журнала 293

RP (восстановление программ, принимающих права доступа), формат файла 695

RPLDOC (Заменить документ), команда
 контроля объекта 546
 необходимые права доступа к объектам 398

RQ (восстановление объекта *CRQD), тип записи журнала 293

RQ (восстановление объекта *CRQD, принимающего права доступа), формат файла 697

RRTJOB (Начать новый шаг задания), команда
необходимые права доступа к объектам 438

RSMBKP (Восстановить точку прерывания), команда
необходимые права доступа к объектам 492

RSMCTLRZY (Возобновить исправление ошибок контроллера), команда
контроль объекта 538
необходимые права доступа к объектам 387

RSMDEVRCY (Возобновить исправление ошибок устройства), команда
контроль объекта 539
необходимые права доступа к объектам 392

RSMLINRCY (Возобновить исправление ошибок линии), команда
контроль объекта 562
необходимые права доступа к объектам 463

RSMNWIRCY (Возобновить исправление ошибок сетевого интерфейса), команда
контроль объекта 568

RSTAUT (Восстановить права доступа), команда
запись журнала контроля (QAUDJRN) 293
использование 265
необходимые права доступа к объектам 521
описание 331
пользовательские профайлы, поставляемые IBM, с правами доступа 355
процедура 266
роль в восстановлении защиты 259

RSTCFG (Восстановить конфигурацию), команда
контроль объекта 529
необходимые права доступа к объектам 384
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTDFROBJ (Восстановить отложенный объект), команда
контроль объекта 530

RSTDFROBJ, команда
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTDLO (Восстановить объект библиотеки документов), команда 259
контроль объекта 546
необходимые права доступа к объектам 399
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTLIB (Восстановить библиотеку), команда 259
контроль объекта 529
необходимые права доступа к объектам 458

RSTLIB (Восстановить библиотеку), команда (*продолжение*)
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTLICPGM (Восстановить лицензионную программу), команда
контроль объекта 529
необходимые права доступа к объектам 461
пользовательские профайлы, поставляемые IBM, с правами доступа 355
рекомендации 267
риск нарушения безопасности 267

RSTOBJ (Восстановить объект), команда
использование 259
контроль объекта 529
необходимые права доступа к объектам 366
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTPFRCOL (Восстановить базу данных статистики), команда
необходимые права доступа к объектам 487
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTPFRDTA, команда 355

RSTS36F (Восстановить файл System/36), команда
необходимые права доступа к объектам 410, 515
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTS36FLR (Восстановить папку System/36), команда
необходимые права доступа к объектам 399, 515
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTS36LIBM (Восстановить элементы библиотеки System/36), команда
необходимые права доступа к объектам 458, 515
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTS38AUT (Восстановить права доступа System/38), команда
необходимые права доступа к объектам 469
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTS3HF (Восстановить книжную полку), команда
контроль объекта 546

RSTSYSINF
необходимые права доступа к объектам 367

RSTUSFCNR (Восстановить контейнер USF), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RSTUSRPRF (Восстановить пользовательский профайл), команда
контроль объекта 589
необходимые права доступа к объектам 521
описание 259, 331
пользовательские профайлы, поставляемые IBM, с правами доступа 355

RTVAUTLE (Получить запись списка прав доступа), команда
контроль объекта 531
необходимые права доступа к объектам 376
описание 327

RTVBCKUP (Получить опции резервного копирования), команда
необходимые права доступа к объектам 477

RTVBNDSRC (Получить исходный файл редактора связей), команда
*SRVPGM, получение экспорта 470
контроль объекта 532, 564, 583
необходимые права доступа к объектам 470

RTVCFGSRC (Получить исходный текст конфигурации), команда
контроль объекта 536, 537, 538, 539, 562, 567, 568
необходимые права доступа к объектам 384

RTVCFGSTS (Получить состояние конфигурации), команда
контроль объекта 538, 539, 562, 568
необходимые права доступа к объектам 384

RTVCLDSRC (Получить исходный текст для локали C), команда
контроль объекта 534

RTVCLNUP (Получить список очистки), команда
необходимые права доступа к объектам 477

RTVCLSRC (Получить исходный текст на CL), команда
контроль объекта 571
необходимые права доступа к объектам 492

RTVCURDIR (Получить текущий каталог), команда
контроль объекта 540
необходимые права доступа к объектам 429

RTVDLONAM (Получить имя объекта библиотеки документов), команда
необходимые права доступа к объектам 399

RTVDOC (Получить документ), команда
контроль объекта 544, 546
необходимые права доступа к объектам 399

- RTVDSKINF (Получить информацию о работе дисков), команда
необходимые права доступа к объектам 477
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- RTVDTAARA (Получить область данных), команда
контроля объекта 547
необходимые права доступа к объектам 389
- RTVGRPA (Получить атрибуты группы), команда
объект, права доступа, необходимые 512
- RTVIMGCLG, команда
необходимые права доступа к объектам 414
- RTVJOBA (Получить атрибуты задания), команда
необходимые права доступа к объектам 439
- RTVLIBD (Получить описание библиотеки), команда
необходимые права доступа к объектам 458
- RTVMBRD (Получить описание элемента), команда
контроля объекта 553
необходимые права доступа к объектам 410
- RTVMSG (Получить сообщение), команда
контроля объекта 565
- RTVNETA (Получить сетевые атрибуты), команда
необходимые права доступа к объектам 471
- RTVOBJD (Получить описание объекта), команда
контроля объекта 530
необходимые права доступа к объектам 367
- RTVPDGRPF (Получить профайл группы дескрипторов печати), команда
необходимые права доступа к объектам 489
- RTVPRD (Получить продукт), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- RTVPTF (Получить PTF), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- RTVPWRSCDE (Получить запись расписания включения и выключения питания), команда
необходимые права доступа к объектам 477
- RTVQMFORM (Получить форму управления запросами), команда
контроля объекта 575
необходимые права доступа к объектам 494
- RTVQMQRV (Получить запрос на управление запросом), команда
контроля объекта 574, 575
необходимые права доступа к объектам 494
- RTVS36A (Получить атрибуты System/36), команда
контроля объекта 588
необходимые права доступа к объектам 515
- RTVSMGOBJ (Получить объект управления системами), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- RTVSYVAL (Получить системное значение), команда
необходимые права доступа к объектам 513
- RTVUSRPRF (Получить пользовательский профайл), команда
использование 133
контроля объекта 589
необходимые права доступа к объектам 521
описание 330
- RTVWSCST (Получить объект настройки рабочей станции), команда
контроля объекта 591
необходимые права доступа к объектам 523
- RU (восстановить права доступа пользовательского профайла), формат файла 698
- RU (восстановление прав доступа пользовательского профайла), тип записи журнала 293
- RUNBCKUP (Запустить резервное копирование), команда
необходимые права доступа к объектам 477
- RUNDNSUPD, команда
необходимые права доступа к объектам 401
- RUNLPDA (Выполнить LPDA-2), команда
контроля объекта 561
необходимые права доступа к объектам 504
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- RUNQRY (Запустить запрос), команда
контроля объекта 575
необходимые права доступа к объектам 494
- RUNRNDCCMD, команда
необходимые права доступа к объектам 402
- RUNSMGCMD (Выполнить команду управления системами), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- RUNSMGOBJ (Запустить объект управления системами), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- RUNSQLSTM (Выполнить оператор SQL), команда
необходимые права доступа к объектам 456
- RVKACCAUT (Аннулировать права доступа к коду доступа), команда
контроля объекта 546
необходимые права доступа к объектам 476
- RVKOBAUT (Аннулировать права доступа к объекту), команда 167
использование 177
контроля объекта 529
необходимые права доступа к объектам 367
описание 328
- RVKPUBAUT (Аннулировать общие права доступа), команда
необходимые права доступа к объектам 367
описание 335, 759
пользовательские профайлы, поставляемые IBM, с правами доступа 355
сведения 761
- RVKUSRPMN (Аннулировать права доступа пользователя), команда
контроля объекта 547
необходимые права доступа к объектам 476
описание 332
- RVKWSOAUT (Аннулировать права доступа к объекту рабочей станции), команда
необходимые права доступа к объектам 412
- RZ (изменение основной группы восстановленного объекта), тип записи журнала 293
- RZ (изменение основной группы восстановленного объекта), формат файла 698

S

- SAV (Сохранить), команда
контроля объекта 527, 540, 584, 586
необходимые права доступа к объектам 429
- SAVAPARDTA (Сохранить данные APAR), команда
необходимые права доступа к объектам 504
пользовательские профайлы, поставляемые IBM, с правами доступа 355
- SAVCFG (Сохранить конфигурацию), команда
контроля объекта 538, 539, 561, 567, 568
необходимые права доступа к объектам 384

SAVCHGOBJ (Сохранить измененный объект), команда
 контроля объекта 527
 необходимые права доступа к объектам 367

SAVDLO (Сохранить объект библиотеки документов), команда
 использование 259
 контроля объекта 527, 544
 необходимые права доступа к объектам 399

SAVLIB (Сохранить библиотеку), команда
 использование 259
 контроля объекта 527
 необходимые права доступа к объектам 459

SAVLICPGM (Сохранить лицензионную программу), команда
 контроля объекта 527
 необходимые права доступа к объектам 461
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

SAVOBJ (Сохранить объект), команда
 использование 259
 контроля объекта 527
 необходимые права доступа к объектам 368
 сохранение получателя журнала контроля 312

SAVPRCOL (Сохранить базу данных статистики), команда
 необходимые права доступа к объектам 487
 пользовательские профайлы, поставляемые IBM, с правами доступа 355

SAVPRDTA, команда 355

SAVRSOBJ (Сохранить/Восстановить объект), команда
 необходимые права доступа к объектам 369

SAVRSTCFG (Сохранить/восстановить конфигурацию), команда
 необходимые права доступа к объектам 384

SAVRSTCHG
 пользовательские профайлы, поставляемые IBM, с правами доступа 356

SAVRSTCHG (Сохранить/Восстановить изменения), команда
 необходимые права доступа к объектам 369

SAVRSTDLO (Сохранить/восстановить объект библиотеки документов), команда
 необходимые права доступа к объектам 399

SAVRSTLIB
 пользовательские профайлы, поставляемые IBM, с правами доступа 356

SAVRSTLIB (Сохранить/Восстановить библиотеку), команда
 необходимые права доступа к объектам 459

SAVRSTOBJ
 пользовательские профайлы, поставляемые IBM, с правами доступа 356

SAVS36F (Сохранить файл System/36), команда
 необходимые права доступа к объектам 410, 515

SAVS36LIBM (Сохранить элементы библиотеки System/36), команда
 необходимые права доступа к объектам 410, 460

SAVSAVFDTA (Сохранить данные файла сохранения), команда
 контроля объекта 527
 необходимые права доступа к объектам 410

SAVSECDA (Сохранить данные защиты), команда
 использование 259
 необходимые права доступа к объектам 521
 описание 331

SAVSHF (Сохранить книжную полку), команда
 контроля объекта 528, 544

SAVSTG (Сохранить содержимое памяти), команда
 контроля объекта 530
 необходимые права доступа к объектам 368

SAVSYS (Сохранить систему), команда
 использование 259
 необходимые права доступа к объектам 368
 описание 331

SAVSYSINF
 необходимые права доступа к объектам 369

SBMCRQ (Передать на выполнение запрос на изменение), команда
 контроля объекта 534

SBMDBJOB (Передать на выполнение задания базы данных), команда
 необходимые права доступа к объектам 439

SBMDKTJOB (Передать на выполнение задания дискеты), команда
 необходимые права доступа к объектам 439

SBMFNCJOB (Передать на выполнение финансовое задание), команда
 необходимые права доступа к объектам 412
 пользовательские профайлы, поставляемые IBM, с правами доступа 356

SBMJOB (Передать задание на выполнение), команда
 SECBATCH, меню 752
 необходимые права доступа к объектам 439
 права доступа, проверка 210

SBMNETJOB (Передать на выполнение сетевое задание), команда
 необходимые права доступа к объектам 439

SBMNWSCMD (Передать на выполнение команду сетевого сервера), команда
 необходимые права доступа к объектам 474
 пользовательские профайлы, поставляемые IBM, с правами доступа 356

SBMRJEJOB (Передать на выполнение задание RJE), команда
 необходимые права доступа к объектам 501

SBMRMTCMD (Передать на выполнение удаленную команду), команда
 необходимые права доступа к объектам 383

SD (изменение системного каталога рассылки), тип записи журнала 291

SD (изменить системный каталог рассылки), формат файла 700

SE (изменение записи маршрутизации подсистемы), тип записи журнала 299

SE (изменение записи о выполнении подсистемы), формат файла 702

SECBATCH (Передать отчеты на обработку в пакетном режиме), меню передача отчетов на обработку 752
 планирование отчетов 753

SETATNPGM (Выбрать программу Attention), команда
 задание, инициализация 109
 необходимые права доступа к объектам 492

SETCSTDTA (Задать опции настройки), команда
 необходимые права доступа к объектам 412

SETJOBATR (опции пользователя), параметр
 пользовательский профайл 112

SETMSTK (Задать главный ключ), команда
 необходимые права доступа к объектам 389
 пользовательские профайлы, поставляемые IBM, с правами доступа 356

SETMSTKEY, команда
 необходимые права доступа к объектам 389
 пользовательские профайлы, поставляемые IBM, с правами доступа 356

SETOBJACC (Задать права доступа к объекту), команда
 необходимые права доступа к объектам 369

SETPGMINF (Задать информацию о программе), команда
 необходимые права доступа к объектам 492

SETTAPCGY (Задать категорию магнитной ленты), команда
необходимые права доступа к объектам 465

SETVTMAP (Задать раскладку клавиатуры VT100), команда
STRTCP (Запустить TCP/IP), команда
необходимые права доступа к объектам 517

STRTCPICF (Запустить интерфейс TCP/IP), команда
необходимые права доступа к объектам 517

необходимые права доступа к объектам 517

SETVTTBL (Задать таблицы преобразования VT), команда
необходимые права доступа к объектам 516

SEV (серьезность очереди сообщений), параметр
пользовательский профайл 108

SF (действие над буферным файлом), формат файла 703

SF (изменение буферного файла), тип записи журнала 301

SIGNOFF (Выход из системы), команда
объект, права доступа, необходимые 512

SLTCMD (Выбрать команду), команда
необходимые права доступа к объектам 383

SM (изменение параметров управления системами), формат файла 710

SM (изменение управления системами), тип записи журнала 302

SNA, пользовательский профайл служб рассылки (QSNADS) 339

SNADS (службы рассылки системной сетевой архитектуры)
QSNADS, пользовательский профайл 339

SNDBRKMSG (Отправить прерывающее сообщение), команда
необходимые права доступа к объектам 467

SNDDOC (Отправить документ), команда
контроль объекта 545

SNDDST (Отправить рассылку), команда
контроль объекта 545
необходимые права доступа к объектам 396

SNDDSTQ (Отправить очередь рассылки), команда
необходимые права доступа к объектам 396
пользовательские профайлы, поставляемые IBM, с правами доступа 356

SNDDTAARA (Отправить область данных), команда
контроль объекта 548

SNDEMLIGC (Отправить код эмуляции 3270PC в формате DBCS), команда
необходимые права доступа к объектам 393

SNDFNCIMG (Отправить образ дискеты с финансовой информацией), команда
необходимые права доступа к объектам 412

SNDJRNE (Отправить запись журнала), команда 310
контроль объекта 560
необходимые права доступа к объектам 446

SNDMGRDTA (Отправить переносимые данные), команда
необходимые права доступа к объектам 468

SNDMSG (Отправить сообщение), команда
необходимые права доступа к объектам 467

SNDNETF (Отправить сетевой файл), команда
необходимые права доступа к объектам 471

SNDNETMSG (Отправить сообщение по сети), команда
необходимые права доступа к объектам 471

SNDNETSPLF (Отправить буферный файл по сети), команда
действие, контроль 581
контроль объекта 569
необходимые права доступа к объектам 509
очередь вывода, параметры 222

SNDNWSMSG (Отправить сообщение сетевого сервера), команда
необходимые права доступа к объектам 474

SNDPGMMSG (Отправить программное сообщение), команда
необходимые права доступа к объектам 467

SNDPRD (Отправить продукт), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

SNDPTF (Отправить PTF), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

SNDPTFORD (Отправить заказ на временное исправление программы), команда
необходимые права доступа к объектам 504
пользовательские профайлы, поставляемые IBM, с правами доступа 356

SNDRJECMD (Отправить RJE), команда
необходимые права доступа к объектам 501

SNDRJECMD (Отправить команду RJE), команда
необходимые права доступа к объектам 501

SNDRPY (Отправить ответ), команда
контроль объекта 566
необходимые права доступа к объектам 467

SNDSMGOBJ (Отправить объект управления системами), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

SNDSRVRQS (Отправить запрос на обслуживание), команда
необходимые права доступа к объектам 504
пользовательские профайлы, поставляемые IBM, с правами доступа 356

SNDTCPSPFL (Отправить буферный файл TCP/IP), команда
действие, контроль 581
контроль объекта 591
необходимые права доступа к объектам 516

SNDTCPSPFL (Отправить буферный файл по TCP), команда
необходимые права доступа к объектам 509

SNDUSRMSG (Отправить пользовательское сообщение), команда
необходимые права доступа к объектам 467

SO (действия над пользовательской информацией о защите сервера), формат файла 711

SPCAUT (специальные права доступа), параметр
пользовательский профайл 89
рекомендации 94

SPCENV (специальная среда), параметр
интерактивное задание выполнения 95
рекомендации 94

SQL
защита файлов 251

SRC (системный информационный код) B900 3D10 (ошибка контроля) 70

SRTSEQ (последовательность сортировки), параметр
пользовательский профайл 110

ST (действия сервисных средств), тип записи журнала 301

ST (обращение к сервисным средствам), формат файла 712

STATFS (Показать информацию о смонтированной файловой системе), команда
необходимые права доступа к объектам 472

STRAPF (Запустить Advanced Printer Function), команда
необходимые права доступа к объектам 374, 410

STRASPBAL
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRASPBAL, команда 392

STRBEST (Запустить BEST/1), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRBEST (Запустить планировщик ресурсов Best/1-400), команда
необходимые права доступа к объектам 487

STRBGU (Запустить Business Graphics Utility), команда
необходимые права доступа к объектам 374

STRCBLDBG (Начать отладку COBOL), команда
необходимые права доступа к объектам 456, 492

STRCGU (Запустить CGU), команда
необходимые права доступа к объектам 403

STRCHTSVR (Запустить сервер CHT), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRCLNUP (Начать очистку), команда
необходимые права доступа к объектам 477

STRCLUNOD
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRCLUNOD, команда
необходимые права доступа к объектам 382

STRCMNTRC (Запустить трассировку соединений), команда
необходимые права доступа к объектам 504
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRCMTCTL (Запустить управление фиксацией), команда
необходимые права доступа к объектам 383

STRCPYSCN (Начать копирование экрана), команда
необходимые права доступа к объектам 504

STRCRG
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRCSP (Запустить утилиты CSP/AE), команда
контроля объекта 572

STRDBG (Начать отладку), команда
контроля объекта 551, 571
необходимые права доступа к объектам 492
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRDBGSVR (Запустить сервер отладки), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRDBMON (Включить монитор баз данных), команда
необходимые права доступа к объектам 487

STRDBRDR (Начать чтение базы данных), команда
необходимые права доступа к объектам 496

STRDFU (Запустить DFU), команда
необходимые права доступа к объектам 374, 410

STRDIGQRY (Запрос DIG), команда
необходимые права доступа к объектам 402

STRDIRSHD (Начать работу с теневыми каталогами), команда
необходимые права доступа к объектам 393

STRDIRSHD (Начать теневое копирование каталога), команда
контроля объекта 544

STRDKTRDR (Начать чтение дискеты), команда
необходимые права доступа к объектам 496

STRDKTWTR (Запустить загрузчик дискеты), команда
необходимые права доступа к объектам 524

STRDSKRGZ (Запустить реорганизацию диска), команда
необходимые права доступа к объектам 394

STRDW (Запустить наблюдение за диском), команда
необходимые права доступа к объектам 487
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STREDU (Начать обучение), команда
необходимые права доступа к объектам 477

STREML3270 (Запустить эмуляцию дисплея 3270), команда
необходимые права доступа к объектам 393

STRFMA (Запустить средство управления шрифтами), команда
контроля объекта 557
необходимые права доступа к объектам 403

STRHOSTQRY (Запрос HOST), команда
необходимые права доступа к объектам 402

STRHOSTSVR
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRHOSTSVR (Запустить сервер хоста), команда
необходимые права доступа к объектам 413

STRIDD (Запустить утилиту интерактивного определения данных), команда
необходимые права доступа к объектам 435

STRIDXMON (Запустить монитор индекса), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRIPSIFC (Запустить интерфейс IP для SNA), команда
необходимые права доступа к объектам 373
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRJOBTRC (Начать трассировку заданий), команда
необходимые права доступа к объектам 487
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRJRN (Начать ведение журнала), команда
контроля объекта 529
необходимые права доступа к объектам 430, 446

STRJRNAP (Начать ведение журнала пути доступа), команда
необходимые права доступа к объектам 446

STRJRNLIB (Начать журналирование библиотеки), команда
необходимые права доступа к объектам 446

STRJRNOBJ (Начать ведение журнала объекта), команда
необходимые права доступа к объектам 447

STRJRNPF (Начать ведение журнала физического файла), команда
необходимые права доступа к объектам 447

STRJRNxxx (Начать ведение журнала), команда
контроля объекта 560

STRJW, команда
необходимые права доступа к объектам 487
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRLOGSVR (Запустить сервер протокола задания), команда
необходимые права доступа к объектам 439

STRMGDSYS (Запустить управляемую систему), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 356

STRMGRSRV (Запустить службы управления), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRMOD (Включить режим), команда
контроля объекта 564
необходимые права доступа к
объектам 469

STRMSF (Запустить среду почтового
сервера), команда
необходимые права доступа к
объектам 464
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRNFSSVR (Запустить сервер NFS),
команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRNFSSVR (Запустить сервер сетевой
файловой системы), команда
необходимые права доступа к
объектам 472

STROBJCVN
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STROBJCVN, команда 369

STRPASTHR (Начать сеанс удаленного
входа), команда
контроля объекта 539
необходимые права доступа к
объектам 395

STRPDM (Запустить администратор
разработки программ (PDM)), команда
необходимые права доступа к
объектам 374

STRPEX (Запустить PEX), команда
необходимые права доступа к
объектам 487
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRPFRG
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRPFRG (Показать графики статистики),
команда
необходимые права доступа к
объектам 487

STRPFRT
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRPFRT (Запустить Performance Tools),
команда
необходимые права доступа к
объектам 488

STRPFRTRC (Начать трассировку
параметров производительности),
команда
необходимые права доступа к
объектам 488

STRPFRTRC (Начать трассировку
параметров производительности),
команда (продолжение)
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRPJ (Запустить предварительные
задания), команда
необходимые права доступа к
объектам 439

STRPRTEML (Запустить эмуляцию
принтера), команда
необходимые права доступа к
объектам 393

STRPRTWTR (Запустить загрузчик
принтера), команда
контроля объекта 568, 591
необходимые права доступа к
объектам 525

STRQMQRV (Запустить запрос на
управление запросом), команда
контроля объекта 573, 574, 575
необходимые права доступа к
объектам 494

STRQRY (Запустить запрос), команда
необходимые права доступа к
объектам 495

STRQSH (Запустить QSH), команда
необходимые права доступа к объектам
псевдоним, QSH 493

STRQST (Начать работу с вопросами и
ответами), команда
необходимые права доступа к
объектам 495

STRREXPCC (Запустить процедуру на
REXX), команда
необходимые права доступа к
объектам 456

STRRGZIDX (Запустить реорганизацию
индекса), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRRJESL (Запустить консоль RJE),
команда
необходимые права доступа к
объектам 501

STRRJERDR (Начать чтение RJE), команда
необходимые права доступа к
объектам 501

STRRJESSN (Запустить сеанс RJE),
команда
необходимые права доступа к
объектам 501

STRRJEWTR (Начать запись RJE),
команда
необходимые права доступа к
объектам 501

STRRLU (Запустить утилиту макета
отчета), команда
необходимые права доступа к
объектам 374

STRRMTWTR (Запустить удаленный
загрузчик), команда
действие, контроль 581, 591
контроля объекта 568

STRRMTWTR (Запустить удаленный
загрузчик), команда (продолжение)
необходимые права доступа к
объектам 525

STRS36 (Запустить System/36), команда
контроля объекта 588
пользовательский профайл
специальная среда 94

STRS36MGR (Запустить миграцию
System/36), команда
необходимые права доступа к
объектам 469
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRS38MGR (Начать перенос данных
System/38), команда
необходимые права доступа к
объектам 469
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRSAVSYNC (Задать права доступа к
объекту), команда
необходимые права доступа к
объектам 369

STRSBS (Запустить подсистему), команда
контроля объекта 577
необходимые права доступа к
объектам 512

STRSCHIDX (Запустить индекс поиска),
команда
контроля объекта 578
необходимые права доступа к
объектам 436

STRSDA (Запустить утилиту создания
меню), команда
необходимые права доступа к
объектам 375

STRSEU (Запустить утилиту ввода
исходного кода), команда
необходимые права доступа к
объектам 375

STRSPLRCL, команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 356

STRSQL (Запустить SQL), команда
необходимые права доступа к
объектам 456, 482

STRSRVJOB (Запустить служебное
задание), команда
необходимые права доступа к
объектам 504
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRSST (Запустить Системный
инструментарий), команда
необходимые права доступа к
объектам 504
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRSSYSMGR (Запустить System Manager), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRTCP (Запустить TCP/IP), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRTCPFTP (Запустить FTP TCP/IP),
команда
необходимые права доступа к
объектам 516

STRTCPRFC (Запустить интерфейс TCP/IP),
команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRTCPPTP (Запустить двухточечный
TCP/IP), команда
необходимые права доступа к
объектам 516

STRTCPSPVR (Запустить сервер TCP/IP),
команда
необходимые права доступа к
объектам 517
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRTCPTELN (Запустить TELNET
TCP/IP), команда
необходимые права доступа к
объектам 517

STRTRC (Запустить трассировку), команда
необходимые права доступа к
объектам 504

STRUPDIDX (Запустить обновление
индекса), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRWCH (Начать слежение), команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

STRWCH, команда
необходимые права доступа к
объектам 504

SUPGRPPRF (дополнительные группы),
параметр
пользовательский профайл 105

SV (действие над системным значением),
формат файла 718

SV (действия с системными значениями),
тип записи 299

System/36
перенос
владельцев прав доступа 161
права доступа к удаленному
файлу 160

System/38
защита команд 248

System/38, среда 144

T

TCP/IP
права доступа к объектам,
необходимые для применения
команд 516

TCP/IP (QTCP), пользовательский
профайл 339

TCP/IP (Transmission Control
Protocol/Internet Protocol)
права доступа к объектам,
необходимые для применения
команд 516

TELNET (Запустить TELNET TCP/IP),
команда
необходимые права доступа к
объектам 517

TFRBCHJOB (Перейти к пакетному
заданию), команда
контроля объекта 558
необходимые права доступа к
объектам 439

TFRCTL (Передать управление), команда
необходимые права доступа к
объектам 492
передача принятых прав доступа 157

TFRGRJOB (Перейти к групповому
заданию), команда
необходимые права доступа к
объектам 439
принятые права доступа 158

TFRJOB (Перейти к заданию), команда
контроля объекта 558
необходимые права доступа к
объектам 439

TFRPASTHR (Перейти к удаленному входу
в систему), команда
необходимые права доступа к
объектам 395

TFRSECJOB (Перейти к вспомогательному
заданию), команда
необходимые права доступа к
объектам 439

Token-Ring
права доступа к объектам,
необходимые для применения
команд 464

TRCASPBAL
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

TRCASPBAL, команда 392

TRCCNN (Трассировать ICF), команда
необходимые права доступа к
объектам 505
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

TRCCNN (Трассировать соединение)
необходимые права доступа к
объектам 505

TRCCPIC (Трассировать соединения CPI)
необходимые права доступа к
объектам 505
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

TRCCSP (Трассировать приложение
CSP/AE), команда
контроля объекта 572

TRCINT (Трассировать внутрисистемно),
команда
необходимые права доступа к
объектам 505
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

TRCJOB (Трассировать задание), команда
необходимые права доступа к
объектам 505
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

TRCTCPAPP
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

TRCTCPAPP, команда
необходимые права доступа к
объектам 505

TRMPRTEML (Прервать эмуляцию
принтера), команда
необходимые права доступа к
объектам 393

TRNCKMKSF, команда
необходимые права доступа к
объектам 389

TRNPIN (Преобразовать личный
идентификационный номер), команда
необходимые права доступа к
объектам 389
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

U

uid (номера ИД пользователя)
восстановление 263

UNMOUNT (Удалить смонтированную
файловую систему)
необходимые права доступа к
объектам 519

UNMOUNT (Удалить смонтированную
файловую систему), команда
необходимые права доступа к
объектам 472

UPDDTA (Обновить данные), команда
необходимые права доступа к
объектам 411

UPDPGM (Обновить программу), команда
контроля объекта 532, 564, 571
необходимые права доступа к
объектам 493

UPDPTFINF (Обновить информацию PTF),
команда
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

UPDSRVPGM (Обновить служебную
программу), команда
контроля объекта 532, 564, 583
необходимые права доступа к
объектам 493

USEADPAUT (Применять принятые права доступа), параметр 160
 USER DEF (пользовательские права доступа) 167
 USER, параметр описания задания 216
 USRCLS (класс пользователя), параметр описание 83
 рекомендации 84
 USROPT (опции пользователя), параметр пользовательский профайл 112, 113
 USROPT (опция пользователя), параметр *CLKWD (ключевое слово CL) 112, 113, 114
 *EXPERT (эксперт) 112, 113, 114, 167
 *HLPFULL (полноэкранная справка) 114
 *NOSTSMMSG (сообщение об отсутствии состояния) 114
 *PRTMSG (печать сообщения) 114
 *ROLLKEY (клавиша прокрутки) 114
 *STSMMSG (сообщение о состоянии) 114
 USRPRF (имя), параметр 79

V

VA (изменение списка управления доступом), тип записи журнала 299
 VA (изменение списка управления доступом), формат файла 719
 VC (запуск и завершение соединения), формат файла 720
 VC (начало или завершение соединения), тип записи журнала 289
 VF (закрытие файлов сервера), формат файла 721
 VFYCMN (Проверить соединения), команда
 контроля объекта 538, 539, 561
 необходимые права доступа к объектам 490, 505
 пользовательские профайлы, поставляемые IBM, с правами доступа 357
 VFYIMGCLG, команда
 необходимые права доступа к объектам 414
 VFYLNKLPDA (Проверить линию связи, поддерживающую LPDA-2), команда
 контроля объекта 562
 необходимые права доступа к объектам 505
 пользовательские профайлы, поставляемые IBM, с правами доступа 357
 VFYMSTK (Проверить главный ключ), команда
 необходимые права доступа к объектам 389
 пользовательские профайлы, поставляемые IBM, с правами доступа 357
 VFYYPIN (Проверить личный идентификационный номер), команда
 необходимые права доступа к объектам 389

VFYYPIN (Проверить личный идентификационный номер), команда
 (*продолжение*)
 пользовательские профайлы, поставляемые IBM, с правами доступа 357
 VFYYPRT (Проверить принтер), команда
 необходимые права доступа к объектам 490, 505
 пользовательские профайлы, поставляемые IBM, с правами доступа 357
 VFYYPAT (Проверить магнитную ленту), команда
 необходимые права доступа к объектам 490, 505
 пользовательские профайлы, поставляемые IBM, с правами доступа 357
 VFYTPCPCNN (Проверить соединение TCP/IP), команда
 необходимые права доступа к объектам 517
 VL (превышение числа учетных записей), тип записи 302
 VL (превышено ограничение для учетной записи), формат файла 721
 VN (вход в сеть и выход из нее), формат файла 722
 VN (вход или выход из сети), тип записи журнала 289
 VO (контрольный список), формат файла 723
 VP (ошибка в сетевом пароле), формат файла 725
 VP (ошибка сетевого пароля), тип записи журнала 288
 VR (обращение к сетевому ресурсу), формат файла 726
 VRYCFG (Изменить состояние конфигурации), команда
 контроля объекта 538, 539, 562, 567, 568
 необходимые права доступа к объектам 384
 VS (сеанс сервера), тип записи журнала 289
 VS (сеанс сервера), формат файла 727
 VU (изменение сетевого профайла), формат файла 728
 VU (изменение сетевого профайла), тип записи журнала 299
 VV (изменение состояния обслуживания), тип записи 301
 VV (изменилось состояние службы), формат файла 729

W

WRKACTJOB (Работа с активными заданиями), команда
 необходимые права доступа к объектам 439
 WRKALR (Работа с предупреждениями), команда
 необходимые права доступа к объектам 374
 WRKALRD (Работа с описанием предупреждения), команда
 контроля объекта 531
 WRKALRD (Работа с описаниями предупреждений), команда
 необходимые права доступа к объектам 374
 WRKALRTBL (Работа с таблицами предупреждений), команда
 необходимые права доступа к объектам 374
 WRKALRTBL (Работа с таблицей предупреждений), команда
 контроля объекта 531
 WRKARMJOB, команда
 необходимые права доступа к объектам 439
 WRKASPJOB, команда
 необходимые права доступа к объектам 439
 WRKAUT (Работа с каталогом прав доступа), команда
 необходимые права доступа к объектам 430
 WRKAUT (Работа с правами доступа), команда 167
 контроля объекта 541, 580, 585
 описание 328
 WRKAUTL (Работа со списками прав доступа), команда
 необходимые права доступа к объектам 376
 описание 327
 WRKAUTL (Работа со списком прав доступа), команда
 контроля объекта 532
 WRKBNDDIR (Работа с каталогом связывания), команда
 контроля объекта 532
 необходимые права доступа к объектам 376
 WRKBNDIRE (Работа с записью каталога связывания), команда
 контроля объекта 532
 необходимые права доступа к объектам 376
 WRKCFGL (Работа со списками конфигурации), команда
 необходимые права доступа к объектам 385
 WRKCFGL (Работа со списком конфигурации), команда
 контроля объекта 533
 WRKCFGSTS (Работа с состоянием конфигурации), команда
 контроля объекта 540, 562, 568
 необходимые права доступа к объектам 385
 WRKCHTFMT (Работа с форматами диаграмм), команда
 необходимые права доступа к объектам 377
 WRKCLS (Работа с классами), команда
 необходимые права доступа к объектам 378
 WRKCLS (Работа с классом), команда
 контроля объекта 535

WRKCMD (Работа с командами), команда
необходимые права доступа к
объектам 383

WRKCMD (Работа с командой), команда
контроля объекта 536

WRKCMTDFN (Работа с определением
фиксации), команда
необходимые права доступа к
объектам 383

WRKCNL (Работа со списками
соединений), команда
контроля объекта 536
необходимые права доступа к
объектам 385

WRKCNL (Работа с записями списка
соединений), команда
контроля объекта 536

WRKCNINF (Работа с контактной
информацией), команда
необходимые права доступа к
объектам 496, 505
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

WRKCO (Работа с описаниями классов
обслуживания), команда
контроля объекта 537
необходимые права доступа к
объектам 378

WRKCRQD (Работа с описанием запроса
на изменение), команда
необходимые права доступа к
объектам 377

WRKCRQD (Работа с описаниями
запросов на изменение), команда
контроля объекта 535

WRKCSI (Работа с исходной информацией
связи), команда
контроля объекта 537
необходимые права доступа к
объектам 384

WRKCTLD (Работа с описаниями
контроллеров), команда
контроля объекта 538
необходимые права доступа к
объектам 387

WRKDBFIDD (Работа с файлами базы
данных с помощью IDDU), команда
необходимые права доступа к
объектам 435

WRKDDMF (Работа с файлами
Управления распределенными данными),
команда
необходимые права доступа к
объектам 411

WRKDEV (Работа с описаниями
устройств), команда
контроля объекта 540
необходимые права доступа к
объектам 392

WRKDEVTBL (Работа с таблицами
устройств), команда
необходимые права доступа к
объектам 412
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

WRKDIRE (Работа с записью каталога),
команда
необходимые права доступа к
объектам 393

WRKDIRE (Работа с каталогом), команда
описание 333

WRKDIRLOC (Работа с расположениями
каталогов), команда
необходимые права доступа к
объектам 393

WRKDIRSHD (Работа с теневыми
каталогами), команда
необходимые права доступа к
объектам 393

WRKDOC (Работа с документами),
команда
контроля объекта 545
необходимые права доступа к
объектам 399

WRKDOCLIB (Работа с библиотеками
документов), команда
контроля объекта 547
необходимые права доступа к
объектам 476

WRKDOCPRTQ (Работа с очередью печати
документов), команда
контроля объекта 547
необходимые права доступа к
объектам 476

WRKDPCQ (Работа с очередями рассылки
DSNX/PC), команда
необходимые права доступа к
объектам 396
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

WRKDSKSTS (Работа с состоянием диска),
команда
необходимые права доступа к
объектам 394

WRKDSTL (Работа со списками рассылки),
команда
необходимые права доступа к
объектам 396

WRKDSTQ (Работа с очередью рассылки),
команда
необходимые права доступа к
объектам 396
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

WRKDTAARA (Работа с областями
данных), команда
контроля объекта 548
необходимые права доступа к
объектам 389

WRKDTADCT (Работа со словарями
данных), команда
необходимые права доступа к
объектам 435

WRKDTADFN (Работа с определениями
данных), команда
необходимые права доступа к
объектам 436

WRKDTAQ (Работа с очередями данных),
команда
контроля объекта 549

WRKDTAQ (Работа с очередями данных),
команда (*продолжение*)
необходимые права доступа к
объектам 390

WRKEDTD (Работа с описаниями
формата), команда
контроля объекта 549
необходимые права доступа к
объектам 403

WRKENVVAR (Работа с переменной
среды), команда
необходимые права доступа к
объектам 403

WRKF (Работа с файлами), команда
контроля объекта 553
необходимые права доступа к
объектам 411

WRKFCNARA
пользовательские профайлы,
поставляемые IBM, с правами
доступа 357

WRKFCNARA (Работа с
функциональными областями), команда
необходимые права доступа к
объектам 488

WRKFCT (Работа с таблицами управления
формами), команда
необходимые права доступа к
объектам 501

WRKFLR (Работа с папками), команда
необходимые права доступа к
объектам 399

WRKFNTRSC (Работа с ресурсами
шрифтов), команда
контроля объекта 554
необходимые права доступа к
объектам 373

WRKFORMDF (Работа с определениями
форм), команда
контроля объекта 554
необходимые права доступа к
объектам 373

WRKFSTAF (Работа с функцией
предупреждения FFST), команда
необходимые права доступа к
объектам 505

WRKFSTPCT (Работа с таблицей
управления тестами FFST), команда
необходимые права доступа к
объектам 505

WRKFTR (Работа с фильтрами), команда
контроля объекта 555
необходимые права доступа к
объектам 412

WRKFTRACNE (Работа с записями о
действиях фильтра), команда
контроля объекта 555
необходимые права доступа к
объектам 412

WRKFTRSLTE (Работа с записями о
выборе фильтра), команда
контроля объекта 555
необходимые права доступа к
объектам 412

WRKGGSS (Работа с наборами графических
символов), команда
контроля объекта 555

WRKGSS (Работа с наборами графических символов), команда *(продолжение)* необходимые права доступа к объектам 413

WRKHDWRSC (Работа с аппаратными ресурсами), команда необходимые права доступа к объектам 497

WRKHLDOPTF (Работа с файлами справки по оптической памяти), команда необходимые права доступа к объектам 480

WRKIMGCLG, команда необходимые права доступа к объектам 414

WRKIMGCLGE, команда необходимые права доступа к объектам 414

WRKIPXD, команда 436

WRKJOB (Работа с заданием), команда необходимые права доступа к объектам 439

WRKJOB D (Работа с описаниями заданий), команда контроля объекта 557 необходимые права доступа к объектам 441

WRKJOBLOG (Работа с протоколами заданий), команда необходимые права доступа к объектам 439

WRKJOBQ (Работа с очередью заданий), команда контроля объекта 558 необходимые права доступа к объектам 442

WRKJOBQD (Работа с описанием очереди заданий), команда необходимые права доступа к объектам 442

WRKJOBSCDE (Работа с записями расписания заданий), команда контроля объекта 558 необходимые права доступа к объектам 443

WRKJRN (Работа с журналом), команда использование 312, 319 контроля объекта 560 необходимые права доступа к объектам 447 пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKJRNA (Работа с атрибутами журнала), команда использование 312, 319 контроля объекта 560 необходимые права доступа к объектам 447

WRKJRNRCV (Работа с получателями журнала), команда контроля объекта 560 необходимые права доступа к объектам 448

WRKJVMJOB, команда необходимые права доступа к объектам 437

WRKLANADPT (Работа с адаптерами LAN), команда необходимые права доступа к объектам 464

WRKLIB пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKLIB (Работа с библиотеками), команда необходимые права доступа к объектам 460

WRKLIBPDM пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKLIBPDM (Работа с библиотеками с помощью PDM), команда необходимые права доступа к объектам 375

WRKLICINF (Работа с информацией о лицензии), команда пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKLIND (Работа с описаниями линий), команда контроля объекта 562 необходимые права доступа к объектам 463

WRKLNK (Работа со ссылками), команда контроля объекта 540, 541, 579, 580, 584, 585, 586, 587 необходимые права доступа к объектам 431

WRKM BRPDM (Работа с элементами с помощью PDM), команда необходимые права доступа к объектам 375

WRKMNU (Работа с меню), команда контроля объекта 563 необходимые права доступа к объектам 466

WRKMOD (Работа с модулем), команда необходимые права доступа к объектам 470

WRKMOD (Работа с модулями), команда контроля объекта 564

WRKMODD (Работа с описаниями режимов), команда контроля объекта 564 необходимые права доступа к объектам 469

WRKMSG (Работа с сообщениями), команда контроля объекта 566 необходимые права доступа к объектам 467

WRKMSGD (Работа с описаниями сообщений), команда контроля объекта 565 необходимые права доступа к объектам 467

WRKMSGF (Работа с файлами сообщений), команда контроля объекта 565

WRKMSGF (Работа с файлами сообщений), команда *(продолжение)* необходимые права доступа к объектам 468

WRKMSGQ (Работа с очередями сообщений), команда контроля объекта 566 необходимые права доступа к объектам 468

WRKNAMSMTP (Работа с именами для SMTP), команда объект необходимые права доступа 517

WRKNETF (Работа с сетевыми файлами), команда необходимые права доступа к объектам 471

WRKNETJOB E (Работа с записями сетевых заданий), команда необходимые права доступа к объектам 471

WRKNETTBLE (Работа с записями таблицы сетей), команда необходимые права доступа к объектам 517

WRKNODL (Работа со списком узлов), команда контроля объекта 567 необходимые права доступа к объектам 476

WRKNODLE (Работа с записями списка узлов), команда контроля объекта 567 необходимые права доступа к объектам 476

WRKN TBD (Работа с описанием NetBIOS), команда контроля объекта 567 необходимые права доступа к объектам 471

WRKNWID (Работа с описанием сетевого интерфейса), команда контроля объекта 568 необходимые права доступа к объектам 473

WRKNWSALS (Работа с псевдонимом сетевого сервера), команда необходимые права доступа к объектам 474

WRKNWSCFG, команда необходимые права доступа к объектам 475 пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKNWSD (Работа с описанием сетевого сервера), команда контроля объекта 568 необходимые права доступа к объектам 475

WRKNWSENR (Работа с регистрацией пользователей сетевого сервера), команда необходимые права доступа к объектам 474

WRKNWSSN (Работа с сеансом сетевого сервера), команда
необходимые права доступа к объектам 474

WRKNWSSTG (Работа с областью памяти сетевого сервера), команда
необходимые права доступа к объектам 474

WRKNWSSTS (Работа с состоянием сетевого сервера), команда
необходимые права доступа к объектам 474

WRKOBJ (Работа с объектами), команда
необходимые права доступа к объектам 369
описание 328

WRKOBJCSP (Работа с объектами для CSP/AE), команда
контроля объекта 538, 572

WRKOBJLCK (Работа с блокировками объектов), команда
необходимые права доступа к объектам 369

WRKOBJLCK (Работа с блокировкой объекта), команда
контроля объекта 530

WRKOBJOWN (Работа с объектами по владельцу), команда
использование 171
контроля объекта 530, 590
необходимые права доступа к объектам 369
описание 328
параметров контроля 275

WRKOBJPDM (Работа с объектами с помощью PDM), команда
необходимые права доступа к объектам 375

WRKOBJPGP (Работа с объектами по основной группе), команда 152, 172
необходимые права доступа к объектам 369
описание 328

WRKOPTDIR (Работа с оптическими каталогами), команда
необходимые права доступа к объектам 480

WRKOPTF (Работа с оптическими файлами), команда
необходимые права доступа к объектам 480

WRKOPTVOL (Работа с оптическими томами), команда
необходимые права доступа к объектам 480

WRKORDINF (Работа с информацией о заказе), команда
необходимые права доступа к объектам 518
пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKOUTQ (Работа с очередью вывода), команда
контроля объекта 569
необходимые права доступа к объектам 482

WRKOUTQD (Работа с описанием очереди вывода), команда
защита, параметры 222
контроля объекта 569
необходимые права доступа к объектам 482

WRKOVL (Работа с перекрытиями), команда
контроля объекта 570
необходимые права доступа к объектам 373

WRKPAGDFN (Работа с определениями страниц), команда
контроля объекта 570
необходимые права доступа к объектам 373

WRKPAGSEG (Работа с сегментами страниц), команда
контроля объекта 570
необходимые права доступа к объектам 373

WRKPCLTBLE (Работа с записями таблицы протоколов), команда
необходимые права доступа к объектам 517

WRKPDG (Работа с группой дескрипторов печати), команда
контроля объекта 571

WRKPEXDFN (Работа с определением PEX), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKPEXFTR (Работа с фильтром PEX), команда
пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKPFCSST (Работа с ограничениями физического файла), команда
контроля объекта 553
необходимые права доступа к объектам 411

WRKPGM (Работа с программами), команда
контроля объекта 572
необходимые права доступа к объектам 493

WRKPGMTBL (Работа с таблицами программ), команда
необходимые права доступа к объектам 412
пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKPNLGRP (Работа с группами панелей), команда
контроля объекта 573
необходимые права доступа к объектам 466

WRKPRB (Работа с неполадкой), команда
необходимые права доступа к объектам 490, 505
пользовательские профайлы, поставляемые IBM, с правами доступа 357

WRKPTFGRP (Работа с группами исправлений), команда 358

WRKPTFGRP (Работа с группой PTF), команда
необходимые права доступа к объектам 505

WRKPTFFORD 358

WRKQMFORD (Работа с формой управления запросами), команда
контроля объекта 574
необходимые права доступа к объектам 495

WRKQMORY (Работа с запросом на управление запросом), команда
необходимые права доступа к объектам 495

WRKQRY (Работа с запросом), команда
необходимые права доступа к объектам 495

WRKQST (Работа с вопросами), команда
необходимые права доступа к объектам 495

WRKRDBDIRE (Работа с записями каталога реляционной базы данных), команда
необходимые права доступа к объектам 497

WRKREGINF (Работа с регистрацией), команда
необходимые права доступа к объектам 496

WRKREGINF (Работа с регистрационной информацией), команда
контроля объекта 550

WRKRJESSN (Работа с сеансом RJE), команда
необходимые права доступа к объектам 501

WRKRPYLE (Работа с записями системного списка ответов), команда
контроля объекта 577
необходимые права доступа к объектам 513

WRKS36PGMA (Работа с атрибутами программы System/36), команда
контроля объекта 572
необходимые права доступа к объектам 515

WRKS36PRCA (Работа с атрибутами процедуры System/36), команда
контроля объекта 553
необходимые права доступа к объектам 515

WRKS36SRCA (Работа с атрибутами исходного текста System/36), команда
контроля объекта 553
необходимые права доступа к объектам 515

WRKSBMJOB (Работа с заданиями, переданными на выполнение), команда
необходимые права доступа к объектам 439

WRKSBS (Работа с подсистемами), команда
контроля объекта 578
необходимые права доступа к объектам 512

WRKSBSD (Работа с описаниями подсистем), команда
 контроля объекта 578
 необходимые права доступа к объектам 512

WRKSBSJOB (Работа с заданиями подсистемы), команда
 контроля объекта 578
 необходимые права доступа к объектам 439

WRKSCIDX (Работа с индексами поиска), команда
 контроля объекта 578
 необходимые права доступа к объектам 436

WRKSCIDX (Работа с записями индекса поиска), команда
 контроля объекта 578
 необходимые права доступа к объектам 436

WRKSHRPOOL (Работа с общими пулами памяти), команда
 необходимые права доступа к объектам 512

WRKSOC (Работа со сферой управления), команда
 необходимые права доступа к объектам 508

WRKSPADCT (Работа с орфографическими словарями), команда
 необходимые права доступа к объектам 507

WRKSPLF (Работа с буферными файлами), команда 222
 контроля объекта 569
 необходимые права доступа к объектам 509

WRKSPLFA (Работа с атрибутами буферного файла), команда
 контроля объекта 569

WRKSPTRD (Работа с поддерживаемыми продуктами), команда
 контроля объекта 573

WRKSRVPGM (Работа со служебными программами), команда
 контроля объекта 584
 необходимые права доступа к объектам 493

WRKSRVPVD (Работа с поставщиками служб), команда
 необходимые права доступа к объектам 505
 пользовательские профайлы, поставляемые IBM, с правами доступа 358

WRKSRVTBLE (Работа с записями таблицы служб), команда
 необходимые права доступа к объектам 517

WRKSSND (Работа с описанием сеанса), команда
 необходимые права доступа к объектам 501

WRKSYSACT
 пользовательские профайлы, поставляемые IBM, с правами доступа 358

WRKSYSACT (Работа с операциями системы), команда
 необходимые права доступа к объектам 488

WRKSYSSTS (Работа с состоянием системы), команда 229
 необходимые права доступа к объектам 512

WRKSYSVAL (Работа с системными значениями), команда
 использование 272
 необходимые права доступа к объектам 513

WRKTAPCTG (Работа с кассетой магнитной ленты), команда
 необходимые права доступа к объектам 465

WRKTBL (Работа с таблицами), команда
 контроля объекта 588
 необходимые права доступа к объектам 516

WRKTCPTS (Работа с состоянием сети TCP/IP), команда
 объект, права доступа, необходимые 517

WRKTIMZON, команда 518

WRKTRC, команда
 пользовательские профайлы, поставляемые IBM, с правами доступа 358

WRKTXIDX (Работа с текстовым индексом), команда
 пользовательские профайлы, поставляемые IBM, с правами доступа 358

WRKUSRJOB (Работа с пользовательскими заданиями), команда
 необходимые права доступа к объектам 439

WRKUSRPRF (Работа с пользовательскими профайлами), команда
 использование 122
 контроля объекта 590
 необходимые права доступа к объектам 521
 описание 330

WRKUSRTBL (Работа с таблицами пользователей), команда
 необходимые права доступа к объектам 412
 пользовательские профайлы, поставляемые IBM, с правами доступа 358

WRKWCH, команда
 пользовательские профайлы, поставляемые IBM, с правами доступа 358

WRKWTR (Работа с загрузчиками), команда
 необходимые права доступа к объектам 525

X

X0 (идентификация Kerberos), формат файла 730

Y

YC (изменение объекта DLO), формат файла 738
 YR (чтение объекта DLO), формат файла 739

Z

ZC (изменение объекта), формат файла 740
 ZR (чтение объекта), формат файла 743

A

автоматическая замена получателей 310
 автоматическая настройка (QAUTOCFG), системное значение
 значение, устанавливаемое командой CFGSYSSEC 759
 автоматическая настройка виртуальных устройств (QAUTOVRT), системное значение 41
 значение, устанавливаемое командой CFGSYSSEC 759
 автоматическая настройка устройств (AUTOCFG), значение 40
 автоматическая настройка устройств (QAUTOCFG), системное значение обзор 40
 автоматическая установка (QLPAUTO), пользовательский профайл
 значения по умолчанию 339
 автоматическая установка лицензионной программы, пользовательский профайл (QLPAUTO)
 восстановление 263
 автоматическая установка лицензионных программ (QLPAUTO), пользовательский профайл
 восстановление 263
 автоматическое создание
 пользовательский профайл 77
 администратор защиты (*SECADM), специальные права доступа
 разрешенные функции 90
 активация
 пользовательский профайл 749
 функция контроля за действиями 308
 анализ
 записи журнала контроля 313
 пользовательский профайл
 по классу пользователя 754
 по специальным правам доступа 754
 пользовательских профайлов 320
 права доступа к объектам 321
 программный сбой 322
 анализ неполадки
 атрибут удаленного обслуживания (QRMTSRVATR), системное значение 42
 Анализировать операции профайлов (ANZPRFACT), команда
 описание 749
 создание исключений для пользователей 749

Анализировать пароли по умолчанию (ANZDFTPWD), команда
описание 749

аннулирование
общие права доступа 335, 759
пользователь, права доступа 332
права доступа к объектам 328

Аннулировать общие права доступа (RVKPUBAUT), команда
описание 335, 759
сведения 761

Аннулировать права доступа к объекту (RVKOBJAUT), команда 167, 177, 328

Аннулировать права доступа пользователя (RVKUSRPMN), команда 332

аппаратное обеспечение
права доступа к объектам, необходимые для применения команд 497
расширенная защита памяти 18

атрибут домена, объект
описание 16
просмотр 16

атрибут защиты
права доступа к объектам, необходимые для применения команд 502

атрибут режима
объекта 16

атрибут режима, программа
просмотр 16

атрибут удаленного обслуживания (QRMTSRVATR), системное значение 42

атрибуты журнала
работа с 319

Б

беспроводная локальная сеть, настройка
права доступа к объектам, необходимые для применения команд 403

библиотека
AUTOCFG (автоматическая настройка устройств), значение 40
CRTAUT (права при создании), параметр
описание 146
пример 152
риски 146
указание 165
CRTOBJAUD (контроль создаваемого объекта), значение 74
QRETSVRSEC (сохранить идентификационные данные на сервере), значение 34
QTEMP (временная)
уровень защиты 50 21

автоматическая настройка устройств (AUTOCFG), значение 40

восстановление 259

защита
описание 142
пример 237
принятые права доступа 142
разработка 236

библиотека (*продолжение*)
защита (*продолжение*)
рекомендации 236
риски 141

общие права доступа
указание 165

печать списка описаний подсистем 334

планирование 236

права доступа
новые объекты 146
описание 142
определение 6

права доступа к объектам, необходимые для применения команд 456

права при создании (CRTAUT), параметр
описание 146
пример 152
риски 146
указание 165

принадлежность объекта 255

разработка 236

создание 165

создать контроль за объектом (CRTOBJAUD), значение 74

сохранение 259

сохранить идентификационные данные на сервере (QRETSVRSEC), значение 34

список
все библиотеки 321
содержимое 321
текущая 85

библиотека (*LIB), контроль 561

библиотека документов, контроль за объектом
изменение
описание команды 331

блок-схема
описание устройства, права доступа 212
определение специальной среды 95
права доступа, проверка 178

блокировать (*HOLD), режим доставки пользовательский профайл 107

блокировка
изменение пароля
QPWDCHGBLK, системное значение 51

требование
изменить (системное значение QPWDCHGBLK) 51

большие профайлы
планирование приложений 237

большой пользовательский профайл 321

буфер (QSPL), пользовательский профайл 339

буферизация
клавиатура 98
клавиша Attention 98

буферизация ввода (*TYPEAHEAD), буферизация клавиатуры 99

буферизация клавиатуры
KBDBUF пользовательский профайл, параметр 98

буферизация клавиатуры (*продолжение*)
QKDBBUF, системное значение 99

буферное задание (QSPLJOB), пользовательский профайл 339

буферный файл
*JOBCTL (управление заданиями), специальные права доступа 91
*SPLCTL (управление буфером), специальные права доступа 91
владелец 222
действие, контроль 581
защита 222
изменение
запись журнала контроля (QAUDJRN) 301
копирование 222
перенос 222
права доступа к объектам, необходимые для применения команд 508
просмотр 222
работа с 222
удаление пользовательского профайла 129

В

важные данные
защита 275
шифрование 277

ведение журнала
инструмент защиты 248

виртуальное устройство
автоматическая настройка (системное значение QAUTOVRT) 41
определение 41

виртуальный принтер
защита 227

вирус
обнаружение 277, 322, 330
поиск 322

включен (*ENABLED), состояние пользовательского профайла 83

включение
соединение
запись журнала контроля (QAUDJRN) 289
функция контроля 308

владелец 152
OWNER, параметр пользовательского профайла
описание 150

владелец прав доступа
System/36, перенос данных 161
автоматическое создание 161
восстановление 259
команды 327, 332
контроля объекта 532
описание 160
печать 334
права доступа к объектам, необходимые для применения команд 375
превышение ограничения на объем памяти 152
просмотр 160, 327
риски 162

- владелец прав доступа (*продолжение*)
 - создание 160, 327, 332
 - сохранение 259
 - удаление 161, 327
- владелец, права доступа
 - блок-схема 184
- внутренний управляющий блок
 - запрет на изменение 22
- вопрос и ответ
 - права доступа к объектам, необходимые для применения команд 495
- восстановить
 - риск нарушения безопасности 227
- Восстановить библиотеку (RSTLIB), команда 259
- Восстановить лицензионную программу (RSTLICPGM), команда
 - рекомендации 267
 - риск нарушения безопасности 267
- Восстановить объект (RSTOBJ), команда
 - использование 259
- Восстановить объект библиотеки документов (RSTDLO), команда 259
- восстановить память (QRCL), библиотека QALWUSRDMN (разрешить пользовательские объекты, системное значение 28
- Восстановить память (RCLSTG), команда 21, 152, 269
 - QALWUSRDMN (разрешить пользовательские объекты, системное значение 28
- Восстановить пользовательский профайл (RSTUSRPRF) 259, 331
- Восстановить права доступа (RSTAUT), команда
 - запись журнала контроля (QAUDJRN) 293
 - использование 265
 - описание 331
 - процедура 266
 - роль в восстановлении защиты 259
- восстановить права доступа пользовательского профайла (RU), формат файла 698
- восстановление
 - *ALLOBJ (ко всем объектам), специальные права доступа
 - специальные права доступа ко всем объектам (*ALLOBJ) 263
 - ALWOBJDIF (Разрешить различия в объектах), параметр 264
 - gid (номера ИД группы) 263
 - uid (номера ИД пользователя) 263
 - библиотека 259
 - владелец по умолчанию (QDFTOWN)
 - запись журнала контроля (QAUDJRN) 293
 - владелец прав доступа 259
 - задание, описание
 - запись журнала контроля (QAUDJRN) 293
 - изменение принадлежности
 - запись журнала контроля (QAUDJRN) 293
 - информации о защите 259
- восстановление (*продолжение*)
 - лицензионной программы
 - рекомендации 267
 - риск нарушения безопасности 267
 - максимальный объем памяти (MAXSTG) 99
 - необходимый объем памяти 99
 - общие права доступа 259, 264
 - объект *CRQD
 - запись журнала контроля (QAUDJRN) 293
 - объект *CRQD, принимающий права доступа (RQ), формат файла 697
 - объект библиотеки документов (DLO) 259
 - объекта
 - запись журнала контроля (QAUDJRN) 293
 - команды 259
 - принадлежность 259, 263
 - советы по организации защиты 263
 - ограничение 228
 - операционная система 269
 - основная группа 259, 264
 - память 21, 152, 269
 - QALWUSRDMN (разрешить пользовательские объекты, системное значение 28
 - пароль DST (специальных сервисных средств)
 - запись журнала контроля (QAUDJRN) 294
 - поврежденный журнал контроля 310
 - поврежденный список прав доступа 268
 - пользовательский профайл
 - запись журнала контроля (QAUDJRN) 294
 - описание команды 331
 - процедуры 259, 262
 - пользовательских профайлов 259
 - права доступа
 - запись журнала контроля (QAUDJRN) 293
 - обзор команд 259
 - описание команды 331
 - описание процесса 266
 - процедура 265
 - права доступа, изменяемые системой
 - запись журнала контроля (QAUDJRN) 293
 - принадлежность объекта 259
 - принятые права доступа
 - изменения принадлежности и прав доступа 267
 - проверка программы 18
 - программный сбой
 - запись журнала контроля (QAUDJRN) 293
 - программы 266
 - Разрешить различия в объектах (ALWOBJDIF), параметр 264
 - список прав доступа 259
 - обзор команд 259
 - описание процесса 268
 - связь с объектом 264
- восстановление (*продолжение*)
 - частные права доступа 259, 264
 - восстановление *CRQD (RQ), формат файла 698
 - восстановление объекта (OR), тип записи журнала 293
 - восстановление объекта типа *CRQD (RQ), тип записи журнала 293
 - восстановление описания задания (RJ), тип записи журнала 293
 - восстановление описания задания (RJ), формат файла 692
 - восстановление памяти (QRCLAUTL), список прав доступа 269
 - восстановление прав доступа пользовательского профайла (RU), тип записи журнала 293
 - восстановление программ, принимающих права доступа (RP), формат файла 695
 - восстановление путей доступа
 - действие, контроль 530
 - права доступа к объектам, необходимые для применения команд 371
 - временная (QTEMP), библиотека
 - уровень защиты 50 21
 - временное исправление программы (PTF)
 - права доступа к объектам, необходимые для применения команд 502
 - все (*ALL), права доступа 140, 361
 - Вставить исходный текст, команда
 - необходимые права доступа к объектам 409
 - вход
 - сеть
 - запись журнала контроля (QAUDJRN) 289
 - вход в сеть и выход из нее (VN), формат файла 722
 - вход в систему
 - без ИД пользователя 215
 - без ИД пользователя и пароля 17
 - действие при достижении максимального числа попыток (QMAXSGNACN), системное значение 33
 - защита, проверка 209
 - консоль 213
 - необходимые права доступа 209
 - неправильный ИД пользователя
 - запись журнала контроля (QAUDJRN) 287
 - неправильный пароль
 - запись журнала контроля (QAUDJRN) 287
 - ограничение прав системного администратора 211
 - ограничение числа попыток входа в систему 32
 - по умолчанию, запрет 276
 - пользователь со специальными правами доступа *ALLOBJ, ошибка 211
 - пользователь со специальными правами доступа *SERVICE, ошибка 211

вход в систему (*продолжение*)
 права доступа, ошибки 209
 рабочая станция, необходимые права доступа 211
 системный администратор, ошибка 211
 сотрудник службы поддержки, ошибка 211
 удаленный (системное значение QRMTSIGN) 35

вход в систему, меню
 изменение 214
 просмотр исходного текста 214

вход или выход из сети (VN), тип записи журнала 289

Выбрать программу Attention (SETATNPGM), команда 109

вывод
 права доступа к объектам, необходимые для применения команд 508

вывод на принтер (PO), тип записи журнала 293

вывод на принтер (PO), формат файла 685

вывод, приоритет 229

Вызвать программу (CALL), команда
 передача принятых прав доступа 157

вызов
 программа
 передача принятых прав доступа 157

выключение
 контроль, функция 313
 неактивное задание 29
 отключенное задание 42, 45
 параметров контроля 69
 соединение
 запись журнала контроля (QAUDJRN) 289

выполнение (*EXECUTE), права доступа 138, 360

выход
 сеть
 запись журнала контроля (QAUDJRN) 289

Г

графические операции
 права доступа к объектам, необходимые для применения команд 412

группа
 основной
 введение 6
 права доступа
 просмотр 163

группа (*GROUP), права доступа 163

группа дескрипторов печати (*PDG), контроль 571

группа панелей
 права доступа к объектам, необходимые для применения команд 465

группа панелей (*PNLGRP), контроль 572

группа узлов (*NODGRP), контроль 566

группа, права доступа
 GRPAUT, параметр пользовательского профайла 103, 150, 152
 GRPAUTTP, параметр пользовательского профайла 104, 152
 описание 137
 права доступа, пример проверки 196, 200
 принятые права доступа 157

группа, профайл
 введение 5, 78
 дополнительная
 SUPGRPPRF (дополнительные группы), параметр 105
 защита ресурсов 5, 137
 несколько
 планирование 252
 основной 151
 планирование 252
 параметр пользовательского профайла
 изменения при восстановлении профайла 262
 параметр пользовательского профайла GRPPRF
 изменения при восстановлении профайла 262
 описание 102
 параметров контроля
 *ALLOBJ, специальные права доступа 274
 пароль 274
 членство 274
 пароль 80
 планирование 251
 пользовательский профайл
 описание 102
 принадлежность объекта 150
 присвоение имени 80
 список прав доступа
 сравнение 253
 сравнение
 список прав доступа 253

групповое задание
 принятые права доступа 158

Д

данные защиты
 сохранение 259, 331

данные, права доступа
 определение 138

двухбайтовая кодировка (DBCS)
 права доступа к объектам, необходимые для применения команд 402

действие над буферным файлом (SF), формат файла 703

действие над заданием (JOBACN), сетевой атрибут 225, 277

действие над системным значением (SV), формат файла 718

действие по восстановлению устройства (QDEVRCYACN), системное значение 41
 значение, устанавливаемое командой CFGSYSSEC 759

действие при достижении максимального числа попыток входа в систему (QMAXSGNACN), системное значение
 значение, устанавливаемое командой CFGSYSSEC 759
 описание 33

действие при сбое контроля (QAUDENDACN), системное значение 69, 307

действие, контроль
 буферные файлы 581
 восстановление путей доступа 530
 определение 278
 планирование 278
 почтовые службы 562
 Сервер каталогов 542
 службы Office 562
 список ответов 576

действия над пользовательской информацией о защите сервера (SO), формат файла 711

действия по обмену данными между процессами (IP), формат файла 648

действия правил обработки пакетов IP (IR), формат файла 649

действия с почтой (ML), тип записи журнала 291

действия с почтой (ML), формат файла 664

действия сервисных средств (DST), тип записи журнала 301

дескриптор
 задание
 запись журнала контроля (QAUDJRN) 298

диалоговое обучение
 права доступа к объектам, необходимые для применения команд 476

диск
 ограничение использования (MAXSTG), параметр 99

дискета
 права доступа к объектам, необходимые для применения команд 464
 длина пароля 53, 54
 Добавить запись каталога (ADDDIRE), команда 333
 Добавить запись расписания заданий (ADDJOBSCDE), команда
 SECBATCH, меню 753
 Добавить запись списка библиотек (ADDLIBLE), команда 218, 221
 Добавить запись списка прав доступа (ADDAUTLE), команда 175, 327
 Добавить запись таблицы ключей Kerberos (ADDKRBKTE), команда
 необходимые права доступа к объектам 448
 Добавить паспорт Kerberos (ADDKRBTKT), команда
 необходимые права доступа к объектам 448
 Добавить пользователя, меню
 пример 123

Добавить права доступа к объекту библиотеки документов (ADDDLOAUT), команда 332

добавление

- библиотека, запись списка 218, 221
- запись идентификации сервера 332
- запись каталога 333
- пользовательских профайлов 123
- права доступа к объекту библиотеки документов (DLO) 332
- права доступа пользователя 168
- список прав доступа
 - записи 175, 327
 - объекты 176
 - пользователи 175, 327

добавление (*ADD), права доступа 138, 360

документ

- QDOC, профайл 339
- восстановление 259
- объект библиотеки документов (DLO) 259
- пароль
 - изменения при восстановлении профайла 262
- пароль (DOCPWD, параметр пользовательского профайла) 106
- права доступа к объектам, необходимые для применения команд 396
- сохранение 259

домашний каталог (HOMEDIR), параметр пользовательский профайл 115

дополнительная группа

- планирование 252

дополнительные группы

- SUPGRPPRF пользовательский профайл, параметр 105

доставка (DLVRY), параметр пользовательский профайл 107

доступ

- запрет
 - неподдерживаемый интерфейс 16
 - несанкционированный 276
- ограничение
 - консоль 272
 - рабочие станции 272

доступ к DDM (DDMACC), сетевой атрибут 277

доступ к PC Support (PCSACC), сетевой атрибут 277

доступность 1

Ж

журнал

- контроль (QAUDJRN)
 - введение 277
- права доступа к объектам, необходимые для применения команд 443
- применение для контроля за защитой 318
- просмотр
 - контроль операций с файлами 248, 319
 - работа с 319

журнал (*продолжение*)

- управление 311

журнал (*JRN), контроль 559

журнал контроля 309

- печать записей 754
- просмотр записей 334
- работа с 312

журнал контроля действий

- печать записей 754
- просмотр записей 334

журнал контроля, получатель пороговый объем памяти 310

- присвоение имени 309
- создание 309
- сохранение 312

З

завершение

- контроль, функция 313
- параметров контроля 69

Завершить задание (ENDJOB), команда QINACTMSGQ, системное значение 30

загрузка

- записи списка прав доступа 327
- пользовательский профайл 133, 330

Загрузка начальной программы (IPL) *JOBCTL (управление заданиями), специальные права доступа 91

загрузчик

- *JOBCTL (управление заданиями), специальные права доступа 91
- права доступа к объектам, необходимые для применения команд 524

загрузчик принтера

- права доступа к объектам, необходимые для применения команд 524

задание

- дескриптор
 - запись журнала контроля (QAUDJRN) 298
- значения защиты 759
- программа обработки клавиши Attention (ATNPGM) 109
- сетевые атрибуты 335, 759
- системных значений 335, 759
- сокет
 - запись журнала контроля (QAUDJRN) 298

задание дескриптора (GS), тип записи журнала 298

задание, инициализация

- принятые права доступа 211
- программа обработки клавиши Attention 210

задание, описание

- QDFTJOBBD (по умолчанию) 101
- USER, параметр 216
- восстановление
 - запись журнала контроля (QAUDJRN) 293
- защита 17
- защита ресурсов системы 229

задание, описание (*продолжение*)

- изменение
 - запись журнала контроля (QAUDJRN) 298
- отслеживание 275
- печать параметров, влияющих на защиту 754
- по умолчанию (QDFTJOBBD) 101
- пользовательский профайл 101
- права доступа к объектам, необходимые для применения команд 441
- просмотр 276
- рабочая станция, запись 216
- рекомендации 102
- советы по организации защиты 216
- средства связи, запись 216
- уровень защиты 40 17

закрытие файлов сервера (VF), формат файла 721

Заменить журнал (CHGJRN), команда 311, 312

Записи

- записи журнала
 - защита 285
 - параметров контроля 285
- Записи журнала
 - контроль действий 285
- Записи журнала контроля 285
- запись журнала
 - отправка 310
- запись идентификации сервера
 - добавление 332
 - изменение 332
 - удаление 332
- запись каталога
 - добавление 333
 - изменение 333
 - удаление 333
 - удаление пользовательского профайла 127
- запись маршрутизации
 - изменение
 - запись журнала контроля (QAUDJRN) 299
 - права доступа к программе 210
 - производительность 229
- запись удаленного задания (QRJE), пользовательский профайл 339
- запись удаленного задания (RJE)
 - права доступа к объектам, необходимые для применения команд 498

запрет

- вход в систему без ИД и пароля пользователя 276

доступ

- DDM, запрос (DDM) 227
- iSeries Access 226
- изменение внутренних управляющих блоков 22
- несанкционированный доступ 276
- несанкционированный доступ к программам 277
- производительность, злоупотребление 229
- тривиальные пароли 50, 273

запрет (*продолжение*)
удаленное задание, запуск 225

запрет повторяющихся символов в пароле (QPWDLMTREP), системное значение 56

запретить (*EXCLUDE), права доступа 140

запретить некоторые символы (QPWDLMTCHR), системное значение 55

запретить повторяющиеся символы (QPWDLMTREP), системное значение 56

запрещенная команда
запись журнала контроля (QAUDJRN) 292

запрос
анализ записей журнала контроля 315

запрос Query Manager (*QMQR), контроль 574

запуск и завершение соединения (VC), формат файла 720

запуск, приоритет 229

Запустить QSH (STRQSH), команда
необходимые права доступа к объектам псевдоним, QSH 493

Запустить System/36 (STRS36), команда
пользовательский профайл
специальная среда 94

защита
Common Criteria
описание 7

буферный файл 222

важные файлы 248

включение
задания 209
интерактивное задание 209
пакетное задание 210

задание, описание 216

исходные файлы 255

ключ 2

необходимость 1

носитель резервной копии 272

общие рекомендации 232

описание подсистемы 215

очередь вывода 221

планирование 1

принтер, вывод 221, 222

разработка 231

расширенная аппаратная, память 18

системных значений 3

списки библиотек 218

средства 334

физическая 2

цель
доступность 1
конфиденциальность 1
целостность 1

защита (*SECURITY), уровень контроля 297

защита Common Criteria
описание 7

защита на уровне записей 248

защита на уровне полей 248

защита ресурсов
введение 5
ограничение доступа 257

защита ресурсов (*продолжение*)
определение 137

защита с помощью ключа 2

защита файлов
SQL 251

защита, команда
list 327

значение защиты
задание 759

И

игнорирование
принятые права доступа 160

ИД пользователя
DST (специальные сервисные средства)
изменение 135

ошибка
запись журнала контроля (QAUDJRN) 287

ИД пользователя из цифр 79

идентификатор набора символов
CCSID пользовательский профайл,
параметр 111

QCCSID, системное значение 112

идентификатор страны или региона
CNTRYID пользовательский профайл,
параметр 111

QCNTYID, системное значение 111

идентификатор языка
LANGID пользовательский профайл,
параметр 111

QLANGID, системное значение 111

SRTSEQ пользовательский профайл,
параметр 110

идентификация Kerberos (X0), формат файла 730

изменение
DST (специальные сервисные средства),
ИД пользователя 135

job
запись журнала контроля (QAUDJRN) 289
принятые права доступа 158

QAUDCTL (управление контролем),
системное значение 334

QAUDLVL (уровень контроля),
системное значение 334

библиотека документов, контроль за объектом
описание команды 331

буферный файл
запись журнала контроля (QAUDJRN) 301

задание, описание
запись журнала контроля (QAUDJRN) 298

запись идентификации сервера 332

запись каталога 333

запись маршрутизации
запись журнала контроля (QAUDJRN) 299

ИД пользователя
DST (специальные сервисные средства) 135

изменение (*продолжение*)
изменение
запись журнала контроля (QAUDJRN) 298

код учета ресурсов 105

команда
ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
значения по умолчанию 248

контроль действий 334, 751

контроля объекта 93, 328, 332
описание команды 331

меню
PRDLIB (рабочая библиотека),
параметр 220
риск нарушения безопасности 220

объект IPC
запись журнала контроля (QAUDJRN) 298

объект библиотеки документов (DLO)
владелец 332
основная группа 332
права доступа 332

объект, владелец 171, 328

описание устройства
владелец 213

основная группа 152, 328
запись журнала контроля (QAUDJRN) 298

основная группа, восстановление
запись журнала контроля (QAUDJRN) 293

очередь вывода 222

параметров контроля
описание команды 328, 331

пароли пользовательских профайлов,
поставляемых IBM 134

пароль
DST (специальные сервисные средства) 135, 329

IBM, поставляемые
пользовательские профайлы 134

описание 329

применение пароля, системные значения 50

указание пароля, совпадающего с именем пользователя 81

пароль DST (специальных сервисных средств) 135

получатель журнала контроля 311, 312

пользовательский профайл
запись журнала контроля (QAUDJRN) 294

описания команд 329, 330

состав пароля, системные значения 50

способы 127

указание пароля, совпадающего с именем пользователя 81

права доступа
запись журнала контроля (QAUDJRN) 297

описание команды 328

процедуры 167

изменение (*продолжение*)

- права доступа пользователя
- список прав доступа 175
- принадлежность
 - описание устройства 213
- принадлежность объекта
 - перенос приложений в рабочую среду 255
- принятие прав доступа программой
 - запись журнала контроля (QAUDJRN) 298
- принятые права доступа
 - необходимые права доступа 158
- программа
 - настройка параметра USEADPAUT 160
- профайл 330
- сетевой атрибут
 - запись журнала контроля (QAUDJRN) 298
 - связанный с защитой 225
- сетевой профайл
 - запись журнала контроля (QAUDJRN) 299
- системная библиотека, список 218, 239
- системное значение
 - запись журнала контроля (QAUDJRN) 299
- системный каталог
 - запись журнала контроля (QAUDJRN) 291
- список активных профайлов 749
- список библиотек 218
- список прав доступа
 - запись 327
 - права доступа пользователя 175
- список управления доступом
 - запись журнала контроля (QAUDJRN) 299
- средства контроля пользователей 93, 330, 331
- текущая библиотека 218, 221
- управление системами
 - запись журнала контроля (QAUDJRN) 302
- уровень защиты (QSECURITY), системное значение
 - с уровня 10 на уровень 20 13
 - с уровня 20 на уровень 30 13
 - с уровня 20 на уровень 40 19
 - с уровня 20 на уровень 50 22
 - с уровня 30 на уровень 20 13
 - с уровня 30 на уровень 40 19
 - с уровня 30 на уровень 50 22
 - с уровня 40 на 20 13
 - с уровня 40 на уровень 30 20
 - с уровня 50 на уровень 40 или 30 22
- изменение (*CHANGE), права доступа 140, 361
- изменение *CRQD (CQ), формат файла 622
- изменение атрибутов (AU), формат файла 611
- изменение буферного файла), тип записи журнала 301
- изменение владельца восстановленного объекта (RO), формат файла 693
- изменение задания (*JOBDDTA), уровень контроля 289
- изменение задания (JS), тип записи журнала 289
- изменение задания (JS), формат файла 655
- изменение записи маршрутизации подсистемы (SE), тип записи журнала 299
- изменение записи о выполнении подсистемы (SE), формат файла 702
- изменение контроля (AD), тип записи журнала 297
- изменение объекта (*OBJALTER), права доступа 138, 360
- изменение объекта (ZC), формат файла 740
- изменение объекта *CRQD (CQ), тип записи журнала 294
- изменение объекта DLO (YC), формат файла 738
- изменение описания задания (JD), тип записи журнала 298
- изменение описания задания (JD), формат файла 654
- изменение основной группы (PG), тип записи журнала 298
- изменение основной группы (PG), формат файла 682
- изменение основной группы восстановленного объекта (RZ), тип записи журнала 293
- изменение основной группы восстановленного объекта (RZ), формат файла 698
- изменение параметров контроля (AD), формат файла 601
- изменение параметров управления системами (SM), формат файла 710
- изменение пользовательского профайла (CP), тип записи журнала 294
- изменение пользовательского профайла (CP), формат файла 618
- изменение пользовательского профайла (NA), тип записи журнала 298
- изменение прав доступа (CA), тип записи журнала 297
- изменение прав доступа (CA), формат файла 612
- изменение прав доступа восстановленного объекта (RA), формат файла 690
- изменение прав доступа к восстановленным объектам (RA), тип записи журнала 293
- изменение принадлежности (IP), тип записи журнала 298
- изменение принадлежности (OW), тип записи журнала 298
- изменение принадлежности (OW), формат файла 675
- изменение принадлежности восстановленного объекта (RO), тип записи журнала 293
- изменение сетевого профайла (VU), тип записи журнала 299
- изменение сетевого профайла (VU), формат файла 728
- изменение сетевых атрибутов (NA), формат файла 665
- изменение системного значения (SV), тип записи журнала 299
- изменение системного каталога рассылки (SD), тип записи журнала 291
- изменение состояния обслуживания (VV), тип записи журнала 301
- изменение списка управления доступом (VA), тип записи журнала 299
- изменение списка управления доступом (VA), формат файла 719
- изменение управления системами (SM), тип записи журнала 302
- изменения буферного файла (*SPLFDTA), уровень контроля 301, 581
- изменилось состояние службы (VV), формат файла 729
- изменить
 - пароль (QPWDCHGBLK системное значение) 51
- Изменить атрибуты буферного файла (CHGSPLFA), команда 222
- Изменить атрибуты группы узлов, команда
 - контроля объекта 566
- Изменить владельца (CHGOWN), команда 171, 328
- Изменить владельца библиотеки (CHGLIBOWN), инструмент 255
- Изменить владельца объекта (CHGOBJOWN), команда 171, 328
- Изменить владельца объекта библиотеки документов (CHGDLOOWN), команда 332
- Изменить задание (CHGJOB), команда
 - принятые права доступа 158
- Изменить запись каталога (CHGDIRE), команда 333
- Изменить запись расписания активации (CHGACTSCDE), команда
 - описание 749
- Изменить запись расписания истечения срока (CHGEXPCDE), команда
 - описание 749
- Изменить запись списка прав доступа (CHGAUTLE), команда
 - использование 175
 - описание 327
- Изменить значение по умолчанию для команды (CHGCMDDFT), команда 248
- Изменить код учета ресурсов (CHGACGCDE), команда 105
- Изменить команду (CHGCMD), команда
 - ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
- Изменить контроль (CHGAUD), команда
 - использование 132
 - описание 328, 331

- Изменить контроль действий (CHGSECAUD), команда описание 334, 751
- Изменить контроль объекта (CHGOBJAUD), команда *AUDIT (контроль), специальные права доступа 93 QAUDCTL (Управление контролем), системное значение 69 описание 328, 331
- Изменить контроль объекта библиотеки документов (CHGDLOAUD), команда *AUDIT (контроль), специальные права доступа 93 QAUDCTL (Управление контролем), системное значение 69 описание 331, 332
- Изменить контроль пользователей (CHGUSRAUD), команда 330 *AUDIT (контроль), специальные права доступа 93 QAUDCTL (Управление контролем), системное значение 69 использование 132 описание 331
- Изменить контроль пользователей, меню 132
- Изменить меню (CHGMNU), команда PRDLIB (рабочая библиотека), параметр 220 риск нарушения безопасности 220
- Изменить основную группу (CHGPGP), команду 172, 328
- Изменить основную группу объекта (CHGOBJPGP), команда 152, 172, 328
- Изменить основную группу объекта библиотеки документов (CHGDLOPGP), команда описание 332
- Изменить очередь вывода (CHGOUTQ), команда 222
- Изменить параметры контроля за действиями (CHGSECAUD) параметров контроля одношаговый 308
- Изменить пароль (CHGPWD), команда описание 329 параметров контроля 273 применение пароля, системные значения 50 указание пароля, совпадающего с именем пользователя 81
- Изменить пароль Kerberos (CHGKRBPWD), команда необходимые права доступа к объектам 448
- Изменить пароль Специальных сервисных средств (CHGDSTPWD), команда 329
- Изменить пользовательский профайл (CHGUSRPRF), команда 330 использование 127 описание 329 состав пароля, системные значения 50 указание пароля, совпадающего с именем пользователя 81
- Изменить права доступа (CHGAUT), команда 167, 328
- Изменить права доступа к объекту библиотеки документов (CHGDLOAUT), команда 332
- Изменить программу (CHGPGM), команда настройка параметра USEADPAUT 160
- Изменить профайл (CHGPRF), команда 127, 330
- Изменить сетевые атрибуты (CHGNETA), команда 225
- изменить системный каталог рассылки (SD), формат файла 700
- Изменить служебную программу (CHGSRVPGM), команда настройка параметра USEADPAUT 160
- Изменить список активных профайлов (CHGACTPRFL), команда описание 749
- Изменить список библиотек (CHGLIBL), команда 218
- Изменить список библиотек (EDTLIBL), команда 218
- Изменить список системных библиотек (CHGSYSLIBL), команда 218, 239
- Изменить текущую библиотеку (CHGCURLIB), команда ограничение 221
- инверсия
page down (*ROLLKEY, опция пользователя) 114
page up (*ROLLKEY, опция пользователя) 114
- индекс поиска
необходимые права доступа к объектам 436
индекс поиска (*SCHIDX), контроль 578
- инструменты защиты
команды 334, 749
меню 749
содержимое 334, 749
- интегрированная файловая система
права доступа к объектам, необходимые для применения команд 415
- интерактивное задание
выполнение
SPCENV (специальная среда), параметр 95
защита при запуске 209
- интерактивное определение данных
права доступа к объектам, необходимые для применения команд 435
- интерфейс вызовов
уровень защиты 40 16
- информации о защите
восстановление 259
восстановление после сбоя 259
резервное копирование 259
сохранение 259
формат хранения в системе 260
формат хранения на носителе 261
хранение в системе 260
хранение на носителе 261
- информация о входе в систему
просмотр
DSPSGNINF пользовательский профайл, параметр 96
QDSPSGNINF, системное значение 29
- Информация о входе в систему
DSPSGNINF пользовательский профайл, параметр 95
пример 29
сообщение об истечении срока действия пароля 51, 52, 82
- информация о заказе на обновление
права доступа к объектам, необходимые для применения команд 518
- информация, индекс поиска
необходимые права доступа к объектам 436
- использование (*USE), права
доступа 140, 361
- истечение срока хранения
пароль (QPWDEXPITV системное значение) 51
пароль (QPWDEXPWPN системное значение) 52
пользовательский профайл
задание расписания 749
просмотр расписания 749
- исходная информация связи
права доступа к объектам, необходимые для применения команд 383
- исходная информация связи (*CSI), контроль 537
- исходный файл
защита 255

К

- кассета
права доступа к объектам, необходимые для применения команд 464
- кассета магнитной ленты
права доступа к объектам, необходимые для применения команд 464
- каталог
защита 144
права доступа 6
новые объекты 147
права доступа к объектам, необходимые для применения команд 378, 393, 414, 415
работа с 333
- каталог (*DIR), контроль 540
- каталог APPN (ND), формат файла 665
- каталог SQL 251
- каталог рассылки
изменение
запись журнала контроля (QAUDJRN) 291
- каталог рассылки, системный
команды 333

- каталог связывания
 - права доступа к объектам, необходимые для применения команд 376
- каталог связывания, контроль за объектом 532
- квант времени 229
- клавиша Attention (ATTN), буферизация 98
- клавиша page down
 - инверсия (*ROLLKEY, опция пользователя) 114
- клавиша page up
 - инверсия (*ROLLKEY, опция пользователя) 114
- клавиша прокрутки (*ROLLKEY), опция пользователя 114
- класс
 - взаимосвязь с защитой 229
 - права доступа к объектам, необходимые для применения команд 377
- класс (*CLS), контроль 535
- класс обслуживания, описание
 - права доступа к объектам, необходимые для применения команд 378
- класс пользователя
 - анализ назначения 754
- класс пользователя (USRCLS), параметр
 - описание 83
 - рекомендации 84
- класс, пользователь 83
- кластер
 - права доступа к объектам, необходимые для применения команд 378
- клиент, обработка запросов, сетевой атрибут PCSACC 226
- ключ
 - параметров контроля 272
- ключ процессора 272
- ключевое слово CL (*CLKWD), опция пользователя 112, 113, 114
- код доступа
 - права доступа к объектам, необходимые для применения команд 476
- код учета ресурсов (ACGCDE), параметр
 - изменение 105
 - пользовательский профайл 105
- команда
 - NLV (национальный язык)
 - защита 248
 - System/38
 - защита 248
 - аннулирование общих прав доступа 335, 759
 - изменение
 - ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
 - PRDLIB (рабочая библиотека), параметр 220
 - значения по умолчанию 248
 - риск нарушения безопасности 220
 - команда (*продолжение*)
 - параметров контроля
 - запись журнала контроля (QAUDJRN) 288
 - планирование защиты 248
 - создание
 - ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
 - команда (*CMD), контроль 535
 - команда (объект типа *CMD)
 - права доступа к объектам, необходимые для применения команд 382
 - Команда ADDDWDFN
 - пользовательские профайлы, поставляемые IBM, с правами доступа 347
 - Команда ADDJWDFN
 - пользовательские профайлы, поставляемые IBM, с правами доступа 347
 - Команда ADDMSTPART
 - пользовательские профайлы, поставляемые IBM, с правами доступа 347
 - Команда ANZCMDPFR
 - пользовательские профайлы, поставляемые IBM, с правами доступа 348
 - Команда ANZOBJCVN
 - необходимые права доступа к объектам 364
 - Команда ANZUSROBJ
 - необходимые права доступа к объектам 364
 - команда APYJRNCHG (Применить занесенные в журнал изменения)
 - контроля объекта 528, 559
 - необходимые права доступа к объектам 443
 - пользовательские профайлы, поставляемые IBM, с правами доступа 348
 - Команда CHGJRNA (Изменить атрибуты журнала)
 - необходимые права доступа к объектам 444
 - пользовательские профайлы, поставляемые IBM, с правами доступа 349
 - Команда CHKMSTKVV
 - пользовательские профайлы, поставляемые IBM, с правами доступа 349
 - Команда CLRMSTKEY (Очистить главный ключ)
 - пользовательские профайлы, поставляемые IBM, с правами доступа 350
 - Команда CPYFCNARA
 - пользовательские профайлы, поставляемые IBM, с правами доступа 350
 - Команда CPYFRMLDIF
 - пользовательские профайлы, поставляемые IBM, с правами доступа 350
 - Команда CPYTOLDIF 350
 - команда ENDSBS (Завершить работу подсистемы)
 - контроля объекта 577
 - необходимые права доступа к объектам 511
 - команда QPWDLMTCHR 82
 - Команда RMVDFRID
 - необходимые права доступа к объектам 366
 - Команда RST (Восстановить)
 - контроля объекта 529, 541, 580, 585, 587
 - необходимые права доступа к объектам 428
 - пользовательские профайлы, поставляемые IBM, с правами доступа 355
 - Команда RSTDFROBJ
 - необходимые права доступа к объектам 366
 - команда RTVJRNE (Восстановить запись журнала)
 - контроля объекта 559
 - необходимые права доступа к объектам 446
 - Команда STRSPLRCL
 - необходимые права доступа к объектам 509
 - Команда Показать описание объекта (DSPOBJD) 328
 - использование 306
 - объект домена 16
 - режим программы 16
 - с помощью файла вывода 321
 - создан 151
 - Команда Работа с пользовательскими профайлами (WRKUSRPRF) 122, 330
 - команда Сохранить библиотеку (SAVLIB) 259
 - команда, CL
 - ADDAUTLE (Добавить запись списка прав доступа) 175, 327
 - ADDIDIRE (Добавить запись каталога) 333
 - ADDDLOAUT (Добавить права доступа к объекту библиотеки документов) 332
 - ADDJOBSCDE (Добавить запись расписания заданий)
 - SECBATCH, меню 753
 - ADDLIBLE (Добавить запись списка библиотек) 218, 221
 - ADDSVRAUTE (Добавить запись идентификации сервера) 332
 - ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
 - ANZDFTPWD (Анализировать пароли по умолчанию)
 - описание 749

- команда, CL (*продолжение*)
- ANZPRFACT (Анализировать операции профайлов)
 - описание 749
 - создание исключений для пользователей 749
 - CALL (Вызвать программу)
 - передача принятых прав доступа 157
 - CFGSYSSEC (Настроить защиту системы)
 - описание 335, 759
 - CHGACGCDE (Изменить код учета ресурсов) 105
 - CHGACTPRFL (Изменить список активных профайлов)
 - описание 749
 - CHGACTSCDE (Изменить запись расписания активации)
 - описание 749
 - CHGAUTLE (Изменить запись списка прав доступа)
 - использование 175
 - описание 327
 - CHGCMMD (Изменить команду)
 - ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
 - CHGCMDDFT (Изменить значение по умолчанию для команды) 248
 - CHGCURLIB (Изменить текущую библиотеку)
 - ограничение 221
 - CHGDIRE (Изменить запись каталога) 333
 - CHGDLOAUD (Изменить контроль объекта библиотеки документов) 332
 - *AUDIT (контроль), специальные права доступа 93
 - QAUDCTL (Управление контролем), системное значение 69
 - CHGDLOAUD (Изменить параметры контроля объекта библиотеки документов)
 - описание 331
 - CHGDLOAUT (Изменить права доступа к объекту библиотеки документов) 332
 - CHGDLOOWN (Изменить владельца объекта библиотеки документов) 332
 - CHGDLOPGP (Изменить основную группу объекта библиотеки документов) 332
 - CHGDSTPWD (Изменить пароль Специальных сервисных средств) 329
 - CHGEXPCDE (Изменить запись расписания истечения срока)
 - описание 749
 - CHGJOB (Изменить задание)
 - принятые права доступа 158
- команда, CL (*продолжение*)
- CHGJRN (Заменить журнал) 311, 312
 - CHGLIBL (Изменить список библиотек) 218
 - CHGMNU (Изменить меню)
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
 - CHGNETA (Изменить сетевые атрибуты) 225
 - CHGOBJAUD (Изменить контроль объекта) 328
 - *AUDIT (контроль), специальные права доступа 93
 - QAUDCTL (Управление контролем), системное значение 69
 - описание 331
 - CHGOBJOWN (Изменить владельца объекта) 171, 328
 - CHGOBJPGP (Изменить основную группу объекта) 152, 172, 328
 - CHGOUTQ (Изменить очередь вывода) 222
 - CHGPGM (Изменить программу)
 - настройка параметра USEADPAUT 160
 - CHGPRF (Изменить профайл) 127, 330
 - CHGPWD (Изменить пароль)
 - описание 329
 - параметры контроля 273
 - применение пароля, системные значения 50
 - указание пароля, совпадающего с именем пользователя 81
 - CHGSECAUD (Изменить контроль действий)
 - описание 334, 751
 - CHGSPLFA (Изменить атрибуты буферного файла) 222
 - CHGSRVPGM (Изменить служебную программу)
 - настройка параметра USEADPAUT 160
 - CHGSVRAUTE (Изменить запись идентификации сервера) 332
 - CHGSYSLIBL (Изменить список системных библиотек) 218, 239
 - CHGUSRAUD (Изменить контроль пользователей) 330
 - *AUDIT (контроль), специальные права доступа 93
 - QAUDCTL (Управление контролем), системное значение 69
 - использование 132
 - описание 331
 - CHGUSRPRF (Изменить пользовательский профайл) 330
 - использование 127
 - описание 329
 - состав пароля, системные значения 50
 - указание пароля, совпадающего с именем пользователя 81
- команда, CL (*продолжение*)
- CHKOBJTG (Проверить целостность объекта)
 - контроль использования 277
 - описание 322, 330, 754
 - CHKPWD (Проверить пароль) 133, 329
 - CPYSPLF (Скопировать буферный файл) 222
 - CRTAUTHLR (Создать владельца прав доступа) 160, 327, 332
 - CRTAUTL (Создать список прав доступа) 174, 327
 - CRTCMD (Создать команду)
 - ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
 - CRTJRN (Создать журнал) 309
 - CRTJRNRCV (Создать получатель журнала) 309
 - CRTLIB (Создать библиотеку) 165
 - CRTMNU (Создать меню)
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
 - CRTOUTQ (Создать очередь вывода) 222, 224
 - CRTUSRPRF (Создать пользовательский профайл)
 - описание 123, 329, 330
 - DLTAUTHLR (Удалить владельца прав доступа) 161, 327
 - DLTAUTL (Удалить список прав доступа) 177, 327
 - DLTJRNRCV (Удалить получатель журнала) 312
 - DLTUSRPRF (Удалить пользовательский профайл)
 - описание 330
 - пример 127
 - принадлежность объекта 150
 - DSPACTPRFL (Показать список активных профайлов)
 - описание 749
 - DSPACTSCD (Показать расписание активации)
 - описание 749
 - DSPAUDJRNE (Показать записи журнала контроля)
 - описание 334, 754
 - DSPAUTHLR (Показать владельца прав доступа) 160, 327
 - DSPAUTL (Показать список прав доступа) 327
 - DSPAUTLDLO (Показать объекты библиотеки документов списка прав доступа) 332
 - DSPAUTLOBJ (Показать объекты списка прав доступа) 176, 327
 - DSPAUTUSR (Показать пользователей с правами доступа)
 - описание 330
 - параметры контроля 320
 - пример 130

- команда, CL (*продолжение*)
- DSPDLOAUD (Показать параметры контроля объекта библиотеки документов) 306, 332
 - DSPDLOAUT (Показать права доступа к объекту библиотеки документов) 332
 - DSPEXPSCD (Показать расписание истечения срока)
 - описание 749
 - DSPJOB (Показать описание задания) 276
 - DSPJRN (Показать журнал)
 - контроль операций с файлами 248, 319
 - пример журнала контроля (QAUDJRN) 313, 314
 - просмотр QAUDJRN (журнала контроля) 278
 - создание файла вывода 315
 - DSPLIB (Показать библиотеку) 321
 - DSPLIBD (Показать описание библиотеки)
 - CRTAUT, параметр 165
 - DSPOBJAUT (Показать права доступа к объекту) 321, 328
 - DSPOBJD (Показать описание объекта) 306, 328
 - объект домена 16
 - режим программы 16
 - с помощью файла вывода 321
 - создан 151
 - DSPPGM (Показать программу)
 - принятые права доступа 159
 - режим программы 16
 - DSPPGMADP (Показать принимающие программы)
 - использование 159, 248
 - описание 331
 - параметров контроля 322
 - DSPSECAUD (Показать параметры контроля действий)
 - описание 751
 - DSPSECAUD (Показать параметры контроля за действиями)
 - описание 334
 - DSPSPLF (Показать буферный файл) 222
 - DSPSRVPGM (Показать служебную программу)
 - принятые права доступа 159
 - DSPUSRPRF (Показать пользовательский профайл)
 - использование 130
 - описание 330
 - с помощью файла вывода 320
 - EDTAUTL (Редактировать список прав доступа) 175, 327
 - EDTDLOAUT (Редактировать права доступа к объекту библиотеки документов) 332
 - EDTLIBL (Изменить список библиотек) 218
 - EDTOBJAUT (Редактировать права доступа к объекту) 167, 328
- команда, CL (*продолжение*)
- ENDJOB (Завершить задание)
 - QINACTMSGQ, системное значение 30
 - GRTOBJAUT (Предоставить права доступа к объекту) 328
 - влияние на существующие права доступа 170
 - несколько объектов 169
 - GRTUSRAUT (Предоставить права доступа пользователю)
 - копирование прав доступа 127
 - описание 330
 - переименование профайла 132
 - рекомендации 173
 - GRTUSRPMN (Предоставить права доступа пользователю) 332
 - PRADPOBJ (Печатать принимающие объекты)
 - описание 754
 - PRTCMNSSEC (Печать параметров защиты средств связи)
 - описание 335, 754
 - PRTJOBDAUT (Печать прав доступа к описаниям заданий) 334
 - описание 754
 - PRTPUBAUT (Печать объектов с общими правами доступа) 334
 - описание 754
 - PRTPVTAUT (Печать частных прав доступа) 334
 - описание 756
 - список прав доступа 754
 - PRTQAUT (Печать прав доступа к очереди)
 - описание 334, 756
 - PRTSBSDAUT (Печатать права доступа к описанию подсистемы)
 - описание 334
 - PRTSBSDAUT (Печать описания подсистемы)
 - описание 754
 - PRTSYSSECA (Печать системных атрибутов защиты)
 - описание 335, 754
 - PRTTRGPGM (Печать программ триггеров)
 - описание 334, 754
 - PRTUSROBJ (Печать пользовательских объектов)
 - описание 334, 754
 - PRTUSRPRF (Печать пользовательского профайла)
 - описание 754
 - QALWUSRDMN (разрешить пользовательские объекты), системное значение 28
 - RCLSTG (Восстановить память) 21, 28, 152, 269
 - RMVAUTLE (Удалить запись списка прав доступа) 175, 327
 - RMVDIRE (Удалить запись каталога) 333
 - RMVDLOAUT (Удалить права доступа к объекту библиотеки документов) 332
- команда, CL (*продолжение*)
- RMVLIB (Удалить запись списка библиотек) 218
 - RMVSVRAUTE (Удалить запись идентификации сервера) 332
 - RSTAUT (Восстановить права доступа)
 - запись журнала контроля (QAUDJRN) 293
 - использование 265
 - описание 331
 - процедура 266
 - роль в восстановлении защиты 259
 - RSTDLO (Восстановить объект библиотеки документов) 259
 - RSTLIB (Восстановить библиотеку) 259
 - RSTLICPGM (Восстановить лицензионную программу)
 - рекомендации 267
 - риск нарушения безопасности 267
 - RSTOBJ (Восстановить объект)
 - использование 259
 - RSTUSRPRF (Восстановить пользовательские профайлы) 259, 331
 - RTVAUTLE (Получить запись списка прав доступа) 327
 - RTVUSRPRF (Получить пользовательский профайл) 133, 330
 - RVKOBJAUT (Аннулировать права доступа к объекту) 177, 328
 - RVKPUBAUT (Аннулировать общие права доступа)
 - описание 335, 759
 - сведения 761
 - RVKUSRPMN (Аннулировать права доступа пользователя) 332
 - SAVDLO (Сохранить объект библиотеки документов) 259
 - SAVLIB (Сохранить библиотеку) 259
 - SAVOBJ (Сохранить объект) 259, 312
 - SAVSECDTA (Сохранить данные защиты) 259, 331
 - SAVSYS (Сохранить систему) 259, 331
 - SBMJOB (Передача задания на выполнение) 210
 - SECBATCH, меню 752
 - SETATNPGM (Выбрать программу Attention) 109
 - SNDJRNE (Отправить запись журнала) 310
 - SNDNETSPLF (Отправить буферный файл по сети) 222
 - STRS36 (Запустить System/36)
 - пользовательский профайл, специальная среда 94
 - TFRCTL (Передать управление)
 - передача принятых прав доступа 157
 - TFRGRPJOB (Перейти к групповому заданию)
 - принятые права доступа 158
 - WRKAUTL (Работа со списками прав доступа) 327
 - WRKDIRE (Работа с каталогом) 333

- команда, CL *(продолжение)*
- WRKJRN (Работа с журналом) 312, 319
 - WRKJRNA ((Работа с атрибутами журнала) 312, 319
 - WRKOBJ (Работа с объектами) 328
 - WRKOBJOWN (Работа с объектами по владельцу)
 - использование 171
 - описание 328
 - параметров контроля 275
 - WRKOBJPGP (Работа с объектами по основной группе) 152, 172
 - описание 328
 - WRKOUTQD (Работа с описанием очереди вывода) 222
 - WRKSPLF (Работа с буферными файлами) 222
 - WRKSYSSTS (Работа с состоянием системы) 229
 - WRKSYSVAL (Работа с системными значениями) 272
 - WRKUSRPRF (Работа с пользовательскими профайлами) 122, 330
 - Аннулировать общие права доступа (RVKPUBAUT)
 - описание 335
 - Аннулировать права доступа к объекту (RVKOBJAUT) 177, 328
 - Аннулировать права доступа пользователя (RVKUSRPMN) 332
 - владельцы прав доступа, таблица 327, 332
 - Восстановить библиотеку (RSTLIB) 259
 - Восстановить лицензионную программу (RSTLICPGM)
 - рекомендации 267
 - риск нарушения безопасности 267
 - Восстановить объект (RSTOBJ)
 - использование 259
 - Восстановить объект библиотеки документов (RSTDLO) 259
 - Восстановить память (RCLSTG) 21, 28, 152, 269
 - Восстановить пользовательские профайлы (RSTUSRPRF) 259, 331
 - Восстановить права доступа (RSTAUT)
 - запись журнала контроля (QAUDJRN) 293
 - использование 265
 - описание 331
 - процедура 266
 - роль в восстановлении защиты 259
 - Выбрать программу Attention (SETATNPGM) 109
 - Вызвать программу (CALL)
 - передача принятых прав доступа 157
 - Добавить запись идентификации сервера (ADDSVRAUTE) 332
 - Добавить запись каталога (ADD DIRE) 333
 - Добавить запись списка библиотек (ADDLIBLE) 218, 221
- команда, CL *(продолжение)*
- Добавить запись списка прав доступа (ADDAUTLE) 175, 327
 - Добавить права доступа к объекту библиотеки документов (ADD DLOAUT) 332
 - Завершить задание (ENDJOB)
 - QINACTMSGQ, системное значение 30
 - Заменить журнал (CHGJRN) 311, 312
 - Запустить System/36 (STRS36)
 - пользовательский профайл, специальная среда 94
 - защита, список 327
 - Изменить атрибуты буферного файла (CHGSPLFA) 222
 - Изменить владельца объекта (CHGOBJOWN) 171, 328
 - Изменить владельца объекта библиотеки документов (CHGDLOOWN) 332
 - Изменить задание (CHGJOB)
 - принятые права доступа 158
 - Изменить запись идентификации сервера (CHGSVRAUTE) 332
 - Изменить запись каталога (CHGDIRE) 333
 - Изменить запись списка прав доступа (CHGAUTLE)
 - использование 175
 - описание 327
 - Изменить значение по умолчанию для команды (CHGCMDDFT) 248
 - Изменить код учета ресурсов (CHGACGCDE) 105
 - Изменить команду (CHGCMDD)
 - ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
 - Изменить контроль объекта (CHGOBJAUD) 328
 - *AUDIT (контроль), специальные права доступа 93
 - QAUDCTL (Управление контролем), системное значение 69
 - описание 331
 - Изменить контроль объекта библиотеки документов (CHGDLOAUD) 332
 - *AUDIT (контроль), специальные права доступа 93
 - QAUDCTL (Управление контролем), системное значение 69
 - описание 331
 - Изменить меню (CHGMNU)
 - PRDLIB (рабочая библиотека), параметр 220
 - риск нарушения безопасности 220
 - Изменить основную группу объекта (CHGOBJPGP) 152, 172, 328
- команда, CL *(продолжение)*
- Изменить основную группу объекта библиотеки документов (CHGDLOPGP) 332
 - Изменить очередь вывода (CHGOUTQ) 222
 - Изменить параметры контроля за действиями (CHGSECAUD)
 - описание 334
 - Изменить пароль (CHGPWD)
 - описание 329
 - параметров контроля 273
 - применение пароля, системные значения 50
 - указание пароля, совпадающего с именем пользователя 81
 - Изменить пароль Специальных сервисных средств (CHGDSTPWD) 329
 - Изменить пользовательский контроль (CHGUSRAUD) 330
 - *AUDIT (контроль), специальные права доступа 93
 - QAUDCTL (Управление контролем), системное значение 69
 - использование 132
 - описание 331
 - Изменить пользовательский профайл (CHGUSRPRF) 330
 - использование 127
 - описание 329
 - состав пароля, системные значения 50
 - указание пароля, совпадающего с именем пользователя 81
 - Изменить права доступа к объекту библиотеки документов (CHGDLOAUT) 332
 - Изменить программу (CHGPGM)
 - настройка параметра USEADPAUT 160
 - Изменить профайл (CHGPRF) 127, 330
 - Изменить сетевые атрибуты (CHGNETA) 225
 - Изменить служебную программу (CHGSRVPGM)
 - настройка параметра USEADPAUT 160
 - Изменить список библиотек (CHGLIBL) 218
 - Изменить список библиотек (EDTLIBL) 218
 - Изменить список системных библиотек (CHGSYSLIBL) 218, 239
 - Изменить текущую библиотеку (CHGCURLIB)
 - ограничение 221
 - имена параметров, отображение (*CLKWD, опция пользователя) 112, 113, 114
 - инструменты защиты 334, 749
 - ключевые слова, отображение (*CLKWD, опция пользователя) 112, 113, 114

команда, CL (продолжение)

Настроить защиту системы (CFGSYSSEC) описание 335
объект библиотеки документов (DLO) таблица 332
отображение ключевых слов (*CLKWD, опция пользователя) 112, 113, 114
Отправить буферный файл по сети (SNDNETSPLF) 222
Отправить запись журнала (SNDJRNE) 310
пароли, таблица 329
Передать задание на выполнение (SBMJOB) 210
Передать управление (TFRCTL) передача принятых прав доступа 157
Перейти к групповому заданию (TFRGRPJOB) принятые права доступа 158
Печатать атрибуты защиты системы (PRTSYSSECA) описание 335
Печатать объекты, доступные всем пользователям (PRTPUBAUT) 334
Печатать параметры защиты средств связи (PRTCMNSEC) описание 335
Печатать пользовательские объекты (PRTUSROBJ) описание 334
Печатать права доступа к описанию подсистемы (PRTSBSDAUT) описание 334
Печатать права доступа к описаниям заданий (PRTJOBDAUT) 334
Печатать права доступа к очереди (PRTQAUT) описание 334
Печатать программы триггера (PRTTRGPGM) описание 334
Печатать частные права доступа (PRTPVTAUT) 334
Показать библиотеку (DSPLIB) 321
Показать буферный файл (DSPSPLF) 222
Показать владельца прав доступа (DSPAUTHLR) 160, 327
Показать журнал (DSPJRN) контроль операций с файлами 248, 319
пример журнала контроля (QAUDJRN) 313, 314
просмотр QAUDJRN (журнала контроля) 278
создание файла вывода 315
Показать записи журнала контроля (DSPAUDJRNE) описание 334
Показать объекты библиотеки документов списка прав доступа (DSPAUTLDLO) 332
Показать объекты списка прав доступа (DSPAUTLOBJ) 176, 327

команда, CL (продолжение)

Показать описание библиотеки (DSPLIB) CRTAUT, параметр 165
Показать описание задания (DSPJOB) 276
Показать описание объекта (DSPOBJD) 306, 328
объект домена 16
режим программы 16
с помощью файла вывода 321
создан 151
Показать параметры контроля за действиями (DSPSECAUD) описание 334
Показать параметры контроля объекта библиотеки документов (DSPDLOAUD) 306, 332
Показать пользователей с правами доступа (DSPAUTUSR) описание 330
параметров контроля 320
пример 130
Показать пользовательский профайл (DSPUSRPRF) использование 130
описание 330
с помощью файла вывода 320
Показать права доступа к объекту (DSPOBJAUT) 321, 328
Показать права доступа к объекту библиотеки документов (DSPDLOAUT) 332
Показать принимающие программы (DSPPGMADP) использование 159, 248
описание 331
параметров контроля 322
Показать программу (DSPPGM) принятые права доступа 159
режим программы 16
Показать служебную программу (DSPSRVPGM) принятые права доступа 159
Показать список прав доступа (DSPAUTL) 327
Получить запись списка прав доступа (RTVAUTLE) 327
Получить пользовательский профайл (RTVUSRPRF) 133, 330
пользовательские профайлы (работа с ними), таблица 330
пользовательские профайлы (связанные), таблица 331
права доступа к объекту, таблица 328
Предоставить пользователю права доступа (GRTUSRAUT) копирование прав доступа 127
описание 330
переименование профайла 132
рекомендации 173
Предоставить права доступа к объекту (GRTOBJAUT) 328
влияние на существующие права доступа 170
несколько объектов 169

команда, CL (продолжение)

Предоставить права доступа пользователю (GRTUSRPMN) 332
Проверить пароль (CHKPWD) 133, 329
Проверить целостность объекта (CHKOBJTG) контроль использования 277
описание 322, 330
Работа с атрибутами журнала (WRKJRNA) 312, 319
Работа с буферными файлами (WRKSPLF) 222
Работа с журналом (WRKJRN) 312, 319
Работа с каталогом (WRKDIRE) 333
Работа с объектами (WRKOBJ) 328
Работа с объектами по владельцу (WRKOBJOWN) использование 171
описание 328
параметров контроля 275
Работа с объектами по основной группе (WRKOBJPGP) 152, 172
описание 328
Работа с описанием очереди вывода (WRKOUTQD) 222
Работа с пользовательскими профайлами (WRKUSRPRF) 122, 330
Работа с системными значениями (WRKSYSVAL) 272
Работа с состоянием системы (WRKSYSSTS) 229
Работа со списками прав доступа (WRKAUTL) 327
разрешено для пользователя с ограниченными возможностями 88
расписание активации 749
Редактировать права доступа к объекту (EDTOBJAUT) 167, 328
Редактировать права доступа к объекту библиотеки документов (EDTDLOAUT) 332
Редактировать список прав доступа (EDTAUTL) 175, 327
системный каталог рассылки, таблица 333
Скопировать буферный файл (CPYSPLF) 222
Создать библиотеку (CRTLIB) 165
Создать владельца прав доступа (CRTAUTHLR) 160, 327, 332
Создать журнал (CRTJRN) 309
Создать команду (CRTCMD) ALWLMTUSR (разрешить для пользователя с ограниченными возможностями), параметр 88
PRDLIB (рабочая библиотека), параметр 220
риск нарушения безопасности 220
Создать меню (CRTMNU) PRDLIB (рабочая библиотека), параметр 220
риск нарушения безопасности 220
Создать очередь вывода (CRTOUTQ) 222, 224

- команда, CL (*продолжение*)
- Создать получатель журнала (CRTJRNRCV) 309
 - Создать пользовательский профайл (CRTUSRPRF)
 - описание 123, 329, 330
 - Создать список прав доступа (CRTAUTL) 174, 327
 - Сохранить библиотеку (SAVLIB) 259
 - Сохранить данные защиты (SAVSECDDTA) 259, 331
 - Сохранить объект (SAVOBJ) 259, 312
 - Сохранить объект библиотеки документов (SAVDLO) 259
 - Сохранить систему (SAVSYS) 259, 331
 - списков прав доступа 327
 - Удалить владельца прав доступа (DLTAUTHLR) 161, 327
 - Удалить запись идентификации сервера (RMVSVRAUTE) 332
 - Удалить запись каталога (RMVDIRE) 333
 - Удалить запись списка библиотек (RMVLIBLE) 218
 - Удалить запись списка прав доступа (RMVAUTLE) 175, 327
 - Удалить получатель журнала (DLTJRNRCV) 312
 - Удалить пользовательский профайл (DLTUSRPRF)
 - описание 330
 - пример 127
 - принадлежность объекта 150
 - Удалить права доступа к объекту библиотеки документов (RMVDLOAUT) 332
 - Удалить список прав доступа (DLTAUTL) 177, 327
- команда, интегрированная файловая система
- CHGAUD (Изменить контроль) использование 132
 - Изменить параметры контроля (CHGAUD) использование 132
- команда, общая
- CHGAUT (Изменить права доступа) 167
 - CHGOWN (Изменить владельца) 171
 - CHGPGP (Изменить основную группу) 172
 - GRTOBJAUT (Предоставить права доступа к объекту) 167
 - RVKOBJAUT (Аннулировать права доступа к объекту) 167
 - WRKAUT (Работа с правами доступа) 167
 - Аннулировать права доступа к объекту (RVKOBJAUT) 167
 - Изменить владельца (CHGOWN) 171
 - Изменить основную группу (CHGPGP) 172
 - Изменить права доступа (CHGAUT) 167
 - Предоставить права доступа к объекту (GRTOBJAUT) 167
- команда, общая (*продолжение*)
- Работа с правами доступа (WRKAUT) 167
- команда, шаблон объекта
- CHGAUD (Изменить контроль) 328
 - описание 331
 - CHGAUT (Изменить права доступа) 328
 - CHGOWN (Изменить владельца) 328
 - CHGPGP (Изменить основную группу) 328
 - DSPAUT (Показать права доступа) 328
 - WRKAUT (Работа с правами доступа) 328
 - Изменить владельца (CHGOWN) 328
 - Изменить основную группу (CHGPGP) 328
 - Изменить параметры контроля (CHGAUD) 328
 - описание 331
 - Изменить права доступа (CHGAUT) 328
 - Показать права доступа (DSPAUT) 328
 - Работа с правами доступа (WRKAUT) 328
- командная строка
- журнал контроля (QAUDJRN), формат файла 615
- командная строка (CD), формат файла 615
- командный процессор QCMD
- программа обработки клавиши Attention 109
 - специальная среда (SPCENV) 94
- команды
- разработка приложений 374
- команды для разработки
- Приложение 374
- команды для разработки приложений 374
- компоновка программных продуктов (*PRDL0D), контроль 573
- конечная точка APPN (NE), формат файла 666
- консоль
- QCONSOLE, системное значение 213
 - QSECOFR (пользовательский профайл системного администратора) 213
 - QSRV (служебный пользовательский профайл) 213
 - QSRVBAS (основной служебный пользовательский профайл) 213
 - ограничение доступа 272
 - права доступа, необходимые для входа в систему 213
- контроллер, описание
- печать параметров, влияющих на защиту 754
 - права доступа к объектам, необходимые для применения команд 386
- контроль (*AUDIT), специальные права доступа
- разрешенные функции 93
 - риски 93
- контроль действий
- настройка 334, 751
 - просмотр 334, 751
- контроль действий (AUDLVL), параметр пользовательский профайл 118
- контроль за действиями
- права доступа к объектам, необходимые для применения команд 502
- контроль за объектом (OBJAUD), параметр
- пользовательский профайл 117
- контроль, функция
- активация 308
 - включение 308
 - завершение 313
- контрольное значение
- запись журнала контроля (QAUDJRN) 292
 - определение 18
- контрольные списки
- пользователь Internet 256
- контрольные списки, создание 256
- контрольные списки, удаление 256
- контрольный журнал (QAUDJRN) 527, 680
- AD (изменение контроля), тип записи 297
 - AD (изменение параметров контроля), формат файла 601
 - AF (отсутствие необходимых прав доступа), формат файла 604
 - AF (ошибка прав доступа), тип записи 292
 - нарушение аппаратной защиты 18
 - нарушение входа в систему по умолчанию 17
 - нарушение запрещенной команды 19
 - нарушение неподдерживаемого интерфейса 19
 - нарушение описания задания 17
 - неподдерживаемый интерфейс 17
 - описание 286
 - проверка программы 19
- AP (принятые права доступа), тип записи 292
- AP (принятые права доступа), формат файла 611
- AU (изменение атрибутов), формат файла 611
- CA (изменение прав доступа), тип записи 297
- CA (изменение прав доступа), формат файла 612
- CD (командная строка), формат файла 615
- CD (текст команды), тип записи 288
- CO (создание объекта), тип записи 151, 288
- CO (создание объекта), формат файла 616
- CP (изменение пользовательского профайла), тип записи 294
- CP (изменение пользовательского профайла), формат файла 618

контрольный журнал (QAUDJRN)

(продолжение)

CQ (изменение *CRQD), формат файла 622
 CQ (изменение объекта *CRQD), тип записи 294
 CU (операции с кластерами), формат файла 622
 CV (проверка соединения), формат файла 624
 CY (настройка шифрования), формат файла 626
 DI (Сервер каталогов), формат файла 629
 DO (операция удаления), тип записи 288
 DO (операция удаления), формат файла 635
 DS (сброс пароля DST), тип записи 294
 DS (сброс поставляемого IBM ИД пользователя сервисных средств), формат файла 637
 EV (переменная среды), формат файла 638
 GR (шаблон записи), формат файла 639
 GS (задание дескриптора), тип записи 298
 GS (предоставить дескриптор), формат файла 644
 IP (действия по обмену данными между процессами), формат файла 648
 IP (изменение принадлежности), тип записи 298
 IP (межпроцессорная связь), тип записи 287
 IR (действия правил обработки пакетов IP), формат файла 649
 IS (управление защитой в Internet), формат файла 651
 JD (изменение описания задания), тип записи 298
 JD (изменение описания задания), формат файла 654
 JS (изменение задания), тип записи 289
 JS (изменение задания), формат файла 655
 KF (файл набора ключей), формат файла 659
 LD (создание и удаление связей, поиск в каталоге), формат файла 663
 ML (действия с почтой), тип записи 291
 ML (действия с почтой), формат файла 664
 NA (изменение сетевых атрибутов), тип записи 298
 NA (изменение сетевых атрибутов), формат файла 665
 ND (каталог APPN), формат файла 665
 NE (конечная точка APPN), формат файла 666
 O1 (доступ к оптической памяти), формат файла 677, 678

контрольный журнал (QAUDJRN)

(продолжение)

O3 (доступ к оптической памяти), формат файла 679
 OM (управление объектами), формат файла 667
 OM (управление объектом), тип записи 291
 OR (восстановление объекта), тип записи 293
 OR (восстановление объекта), формат файла 671
 OW (изменение принадлежности), тип записи 298
 OW (изменение принадлежности), формат файла 675
 PA (принятие прав доступа программой), тип записи 298
 PG (изменение основной группы), тип записи 298
 PG (изменение основной группы), формат файла 682
 PO (вывод на принтер), формат файла 685
 PO (печатаемый вывод), тип записи 293
 PS (смена профайла), тип записи 299
 PS (смена профайла), формат файла 687
 PW (пароль), тип записи 287
 PW (пароль), формат файла 689
 RA (изменение прав доступа восстановленного объекта), формат файла 690
 RA (изменение прав доступа к восстановленным объектам), тип записи 293
 RJ (восстановление описания задания), тип записи 293
 RJ (восстановление описания задания), формат файла 692
 RO (изменение владельца восстановленного объекта), формат файла 693
 RO (изменение принадлежности восстановленного объекта), тип записи 293
 RP (восстановление программ, принимающих права доступа), тип записи 293
 RP (восстановление программ, принимающих права доступа), формат файла 695
 RQ (восстановление объекта *CRQD), тип записи 293
 RQ (восстановление объекта *CRQD, принимающего права доступа), формат файла 697
 RU (восстановить права доступа пользовательского профайла), формат файла 698
 RU (восстановление прав доступа пользовательского профайла), тип записи 293
 RZ (изменение основной группы восстановленного объекта), тип записи 293

контрольный журнал (QAUDJRN)

(продолжение)

RZ (изменение основной группы восстановленного объекта), формат файла 698
 SD (изменение системного каталога рассылки), тип записи 291
 SD (изменить системный каталог рассылки), формат файла 700
 SE (изменение записи маршрутизации подсистемы), тип записи 299
 SE (изменение записи о выполнении подсистемы), формат файла 702
 SF (действие над буферным файлом), формат файла 703
 SF (изменение буферного файла), тип записи 301
 SG, формат файла 707, 709
 SM (изменение параметров управления системами), формат файла 710
 SM (изменение управления системами), тип записи 302
 SO (действия над пользовательской информацией о защите сервера), формат файла 711
 ST (действия сервисных средств), тип записи 301
 ST (обращение к сервисным средствам), формат файла 712
 SV (действие над системным значением), формат файла 718
 SV (действия с системными значениями), тип записи 299
 VA (изменение списка управления доступом), тип записи 299
 VA (изменение списка управления доступом), формат файла 719
 VC (запуск и завершение соединения), формат файла 720
 VC (начало или завершение соединения), тип записи 289
 VF (закрытие файлов сервера), формат файла 721
 VL (превышение числа учетных записей), тип записи 302
 VL (превышено ограничение для учетной записи), формат файла 721
 VN (вход в сеть и выход из нее), формат файла 722
 VN (вход или выход из сети), тип записи 289
 VO (контрольный список), формат файла 723
 VP (ошибка в сетевом пароле), формат файла 725
 VP (ошибка сетевого пароля), тип записи 288
 VR (обращение к сетевому ресурсу), формат файла 726
 VS (сеанс сервера), тип записи 289
 VS (сеанс сервера), формат файла 727
 VU (изменение сетевого профайла), формат файла 728
 VU (изменение сетевого профайла), тип записи 299
 VV (изменение состояния обслуживания), тип записи 301

контрольный журнал (QAUDJRN)
(*продолжение*)

- VV (изменилось состояние службы), формат файла 729
- X0 (идентификация Kerberos), формат файла 730
- YC (изменение объекта DLO), формат файла 738
- YR (чтение объекта DLO), формат файла 739
- ZC (изменение объекта), формат файла 740
- ZR (чтение объекта), формат файла 743
- автоматическая очистка 311
- анализ
 - с помощью запроса 315
- введение 277
- завершение 313
- замена получателя 312
- отключение получателя 311, 312
- ошибки 69
- поврежденный 310
- порог памяти получателя 310
- просмотр записей 278, 313
- расширение уровня контроля (QAUDLVL2), системное значение 72
- системные записи 310
- создание 309
- способы анализа 313
- управление 310
- уровень контроля (QAUDLVL), системное значение 71
- уровень сохранения 70

контрольный список

- права доступа к объектам, необходимые для применения команд 523

контрольный список (*VLDL), контроль 590

контрольный список (VO), формат файла 723

контроля объекта

- *ALRTBL (таблица предупреждений), объект 531
- *AUTHLR (владелец прав доступа), объект 532
- *AUTL (список прав доступа), объект 531
- *BNDDIR (каталог связывания), объект 532
- *CFGL (список конфигурации), объект 533
- *CHTFMT (формат диаграммы), объект 533
- *CLD (описание локали C), объект 534
- *CLS (класс), объект 535
- *CMD (команда), объект 535
- *CNL (список соединений), объект 536
- *COSD (описание класса обслуживания), объект 537
- *CRQD (описание запроса на изменение), объект 534

контроля объекта (*продолжение*)

- *CSI (исходная информация связи), объект 537
- *CSPMAP (список межсистемных продуктов), объект 537
- *CSPTBL (таблица межсистемных продуктов), объект 538
- *CTLD (описание контроллера), объект 538
- *DEVD (описание устройства), объект 539
- *DIR (каталог), объект 540
- *DOC (документ), объект 544
- *DTAARA (область данных), объект 547
- *DTADCT (словарь данных), объект 548
- *DTAQ (очередь данных), объект 548
- *EDTD (описание формата), объект 549
- *EXITRG (запись регистрации точки выхода), объект 549
- *FCT (таблица управления формами), объект 550
- *FILE (файл), объект 550
- *FLR (папка), объект 544
- *FNTRSC (ресурс шрифта), объект 554
- *FORMDF (определение формы), объект 554
- *FTR (фильтр), объект 554
- *GSS (набор графических символов), объект 555
- *IGCDCT (словарь набора двухбайтовых символов), объект 556
- *IGCSRT (сортировка набора двухбайтовых символов), объект 556
- *IGCTBL (таблица набора двухбайтовых символов), объект 556
- *JOB (описание задания), объект 557
- *JOBQ (очередь заданий), объект 557
- *JOBSCD (планировщик заданий), объект 558
- *JRN (журнал), объект 559
- *JRNRCV (получатель журнала), объект 560
- *LIB (библиотека), объект 561
- *LIND (описание линии), объект 561
- *MENU (меню), объект 563
- *MODD (описание режима), объект 563
- *MODULE (модуль), объект 564
- *MSGF (файл сообщений), объект 564
- *MSGQ (очередь сообщений), объект 565
- *NODGRP (группа узлов), объект 566
- *NODL (список узлов), объект 566
- *NTBD (описание NetBIOS), объект 567
- *NWID (сетевой интерфейс), объект 567
- *NWS (описание сетевого сервера), объект 568

контроля объекта (*продолжение*)

- *OUTQ (очередь вывода), объект 568
- *OVL (перекрытие), объект 570
- *PAGDFN (определение страницы), объект 570
- *PAGSEG (сегмент страницы), объект 570
- *PDG (группа дескрипторов печати), объект 571
- *PGM (программа), объект 571
- *PNLGRP (группа панелей), объект 572
- *PRDAVL (уровень готовности продукта), объект 573
- *PRDDFN (определение продукта), объект 573
- *PRDLOD (компоновка программных продуктов), объект 573
- *QMFORM (форма Query Manager), объект 573
- *QMQR (запрос Query Manager), объект 574
- *QRYDFN (определение запроса), объект 575
- *RCT (таблица информационных кодов), объект 576
- *S36 (описание системы S/36), объект 587
- *SBSD (описание подсистемы), объект 577
- *SCHIDX (индекс поиска), объект 578
- *SOCKET (локальный сокет), объект 578
- *SPADCT (орфографический словарь), объект 580
- *SQLPKG (пакет SQL), объект 582
- *SRVPGM (служебная программа), объект 583
- *SSND (описание сеанса), объект 584
- *STMF (поточковый файл), объект 584
- *SVRSTG (область памяти сервера), объект 584
- *SYMLNK (символьная ссылка), объект 586
- *TBL (таблица), объект 588
- *USRIDX (пользовательский индекс), объект 588
- *USRPRF (пользовательский профайл), объект 589
- *USRQ (пользовательская очередь), объект 590
- *USRSPC (пользовательское пространство), объект 590
- *VLDL (контрольный список), объект 590
- библиотека (*LIB), объект 561
- владелец прав доступа (*AUTHLR), объект 532
- группа дескрипторов печати (*PDG), объект 571
- группа панелей (*PNLGRP), объект 572
- группа узлов (*NODGRP), объект 566
- документ (*DOC), объект 544
- журнал (*JRN), объект 559
- запись регистрации точки выхода (*EXITRG), объект 549

контроля объекта *(продолжение)*
запрос Query Manager (*QMQR),
объект 574
изменение
описание команды 328, 331, 332
индекс поиска (*SCHIDX), объект 578
исходная информация связи (*CSI),
объект 537
каталог (*DIR), объект 540
каталог связывания (*BDNDIR),
объект 532
класс (*CLS), объект 535
команда (*CMD), объект 535
компоновка программных продуктов
(*PRDLOD), объект 573
контрольный список (*VLDL),
объект 590
локальный сокет (*SOCKET),
объект 578
меню (*MENU), объект 563
модуль (*MODULE), объект 564
набор графических символов (*GSS),
объект 555
область данных (*DTAARA),
объект 547
область памяти сервера (*SVRSTG),
объект 584
общие операции 527
описание NetBIOS (*NTBD),
объект 567
описание задания (*JOBID),
объект 557
описание запроса на изменение
(*CRQD), объект 534
описание класса обслуживания
(*COSD), объект 537
описание контроллера (*CTLD),
объект 538
описание линии (*LIND), объект 561
описание локали C (*CLD),
объект 534
описание подсистемы (*SBSD),
объект 577
описание режима (*MODD),
объект 563
описание сеанса (*SSND), объект 584
описание сетевого сервера (*NWSD),
объект 568
описание системы S/36 (*S36),
объект 587
описание устройства (*DEV),
объект 539
описание формата (*EDTD),
объект 549
определение 304
определение запроса (*QRYDFN),
объект 575
определение продукта (*PRDDFN),
объект 573
определение страницы (*PAGDFN),
объект 570
определение формы (*FORMDF),
объект 554
орфографический словарь (*SPADCT),
объект 580
очередь вывода (*OUTQ), объект 568
очередь данных (*DTAQ), объект 548

контроля объекта *(продолжение)*
очередь заданий (*JOBQ), объект 557
очередь сообщений (*MSGQ),
объект 565
пакет SQL (*SQLPCK), объект 582
папка (*FLR), объект 544
перекрытие (*OVL), объект 570
планирование 304
планировщик заданий (*JOBSCD),
объект 558
получатель журнала (*JRNRCV),
объект 560
пользовательская очередь (*USRQ),
объект 590
пользовательский индекс (*USRIDX),
объект 588
пользовательский профайл (*USRPRF),
объект 589
пользовательское пространство
(*USRSPC), объект 590
поточный файл (*STMF), объект 584
программа (*PGM), объект 571
просмотр 306
ресурс шрифта (*FNTRSC),
объект 554
сегмент страницы (*PAGSEG),
объект 570
сетевой интерфейс (*NWID),
объект 567
символьная ссылка (*SYMLNK),
объект 586
словарь данных (*DTADCT),
объект 548
словарь набора двухбайтовых
символов (*IGDCT), объект 556
служебная программа (*SRVPGM),
объект 583
сортировка набора двухбайтовых
символов (*IGCSRT), объект 556
список конфигурации (*CFGL),
объект 533
список межсистемных продуктов
(*CSPMAP), объект 537
список прав доступа (*AUTL),
объект 531
список соединений (*CNL),
объект 536
список узлов (*NODL), объект 566
таблица (*TBL), объект 588
таблица информационных кодов
(*RCT), объект 576
таблица межсистемных продуктов
(*CSPTBL), объект 538
таблица набора двухбайтовых
символов (*IGCTBL), объект 556
таблица предупреждений (*ALRTBL),
объект 531
таблица управления формами (*FCT),
объект 570
уровень готовности продукта
(*PRDAVL), объект 573
файл (*FILE), объект 550
файл сообщений (*MSGF), объект 564
фильтр (*FTR), объект 554
форма Query Manager (*QMFORM),
объект 573

контроля объекта *(продолжение)*
формат диаграммы (*CHTFMT),
объект 533
конфигурация
автоматическая
виртуальные устройства (системное
значение QAUTOVRT) 41
права доступа к объектам,
необходимые для применения
команд 384
конфигурация сетевого сервера
права доступа к объектам,
необходимые для применения
команд 475
конфигурация системы
*IOSYSCFG (конфигурация системы),
специальные права доступа 94
Конфигурация системы (*IOSYSCFG),
особые права доступа
разрешенные функции 94
риски 94
конфиденциальность 1
конфиденциальные данные
защита 275
копирование
буферный файл 222
пользовательский профайл 124
права доступа пользователя
описание команды 330
переименование профайла 132
пример 127
рекомендации 173

Л

лицензионной программы
автоматическая установка (QLPAUTO),
пользовательский профайл
описание 339
восстановление
рекомендации 267
риск нарушения безопасности 267
права доступа к объектам,
необходимые для применения
команд 461
установка (QLPINSTALL),
пользовательский профайл
значения по умолчанию 339
логический файл
защита
записи 248
поля 248
локальный сокет (*SOCKET),
контроль 578

М

магнитная лента
защита 272
права доступа к объектам,
необходимые для применения
команд 464

максимальное число попыток входа в систему (QMAXSIGN), системное значение
значение, устанавливаемое командой CFGSYSSEC 759

максимальное число учетных записей превышение
запись журнала контроля (QAUDJRN) 302

максимальный
длина пароля (системное значение QPWDMAXLEN) 54
объем памяти, параметр MAXSTG
владелец прав доступа 152
группа, принадлежность объектов 150
операция восстановления 99
получатель журнала 99
пользовательский профайл 99
параметров контроля 272
размер
контроль (QAUDJRN), получатель журнала 310
число попыток входа в систему (QMAXSIGN), системное значение 272
описание 32

максимальный объем памяти (MAXSTG), параметр
владелец прав доступа
изменение на QDFTOWN (владелец по умолчанию) 152
группа, принадлежность объектов 150
операция восстановления 99
получатель журнала 99
пользовательский профайл 99

межпроцессорная связь
ошибка
запись журнала контроля (QAUDJRN) 287

межпроцессорная связь (IP), тип записи журнала 287

меню
изменение
PRDLIB (рабочая библиотека), параметр 220
риск нарушения безопасности 220
инструменты защиты 749
начальный 87
пользовательский профайл 87
права доступа к объектам, необходимые для применения команд 465
разработка схемы защиты 240
создание
PRDLIB (рабочая библиотека), параметр 220
риск нарушения безопасности 220
меню (*MENU), контроль 563
меню SECTOOLS (Инструменты защиты) 749
меню Инструмент защиты (SECTOOLS) 749
меню Показать список прав доступа отображение сведений (*EXPERT, опция пользователя) 112, 113, 114

Меню Работа с пользовательскими профайлами 122

меню Редактировать список прав доступа отображение сведений (*EXPERT, опция пользователя) 112, 113, 114

Меню Системный запрос ограничить сеансы одним устройством (LMTDEVSSN) 98

минимальная длина пароля (QPWDMINLEN), системное значение 53

модельный объект 173

модуль
каталог связывания 470
права доступа к объектам, необходимые для применения команд 470

модуль (*MODULE), контроль 564

мост VM/MVS (QGATE), пользовательский профайл 339

Н

набор графических символов
права доступа к объектам, необходимые для применения команд 413

набор графических символов (*GSS), контроль за объектом 555

нарушение описания задания
запись журнала контроля (QAUDJRN) 17

Настроить защиту системы (CFGSYSSEC), команда
описание 335, 759

настройка
значения защиты 759
контроль действий 334, 751
функция контроля 308

настройка шифрования (CY), формат файла 626

национальный язык (NLV)
защита команд 248

начало или завершение соединения (VC), тип записи журнала 289

начальное меню
*SIGNOFF 87
запрет показа 87
изменение 87
пользовательский профайл 87
рекомендация 88

начальное меню (INLMNU), параметр
пользовательский профайл 87

начальный список библиотек
взаимосвязь со списком библиотек задания 218
описание задания (JOBID)
пользовательский профайл 101
рекомендации 221
риски 221
текущая библиотека 85

неактивное задание
сообщение (CPI1126) 30

неактивный
job
очередь сообщений (QINACTMSGQ), системное значение 30
тайм-аут (QINACTIVT), системное значение 29
пользователь
список 320

неподдерживаемый интерфейс
запись журнала контроля (QAUDJRN) 17, 292

неполадка
права доступа к объектам, необходимые для применения команд 489

неполное (*PARTIAL), ограничить возможности 88

неправильный ИД пользователя
запись журнала контроля (QAUDJRN) 287

неправильный пароль
запись журнала контроля (QAUDJRN) 287, 288

несанкционированный
программы 277

несколько групп
планирование 252
пример 203

новый объект
права доступа
CRTAUT (права при создании), параметр 146, 165
GRPAUT (права доступа группы), параметр 103, 150
GRPAUTTYR (тип прав доступа группы), параметр 104
права доступа (системное значение QCRTAUT) 28
права доступа (системное значение QUSEADPAUT) 38
права доступа, пример 152
принадлежность, пример 152

номер ИД группы (gid)
восстановление 263

номер ИД пользователя (uid)
восстановление 263

номер ИД пользователя, параметр
пользовательский профайл 114

носитель
права доступа к объектам, необходимые для применения команд 464

носитель резервной копии
защита 272

О

область данных
права доступа к объектам, необходимые для применения команд 389

область памяти сервера (*SVRSTG), объект 584

обмен сообщениями (iSeries Access)
защита 227

- обновление (*UPD), права доступа 138, 360
- образ
 - права доступа к объектам, необходимые для применения команд 414
- обращение к объекту (*OBJREF), права доступа 138, 360
- обращение к сервисным средствам (ST), формат файла 712
- обращение к сетевому ресурсу (VR), формат файла 726
- обслуживание, базовый пользовательский профайл (QSRVBAS) 339
- общая база данных, пользовательский профайл (QDBSHR) 339
- общая папка
 - защита 227
- общие права доступа
 - аннулирование 335, 759
 - аннулирование с помощью команды RVKPUBAUT 761
 - библиотека 165
 - блок-схема 190
 - восстановление 259, 264
 - новые объекты
 - описание 146
 - указание 165
 - определение 137
 - печать 756
 - пользовательский профайл
 - рекомендация 117
 - права доступа, пример проверки 198, 201
 - сохранение 259
- объединение специальных прав доступа 253
- объект IPC
 - изменение
 - запись журнала контроля (QAUDJRN) 298
- объект библиотеки документов контроля объекта 544
- объект библиотеки документов (DLO)
 - добавление прав доступа 332
 - изменение владельца 332
 - изменение основной группы 332
 - изменение прав доступа 332
 - команды 332
 - права доступа к объектам, необходимые для применения команд 396
 - просмотр прав доступа 332
 - просмотр списка прав доступа 332
 - редактирование прав доступа 332
 - удаление прав доступа 332
- объект домена
 - определение 16
 - просмотр 16
- объект настройки рабочей станции
 - права доступа к объектам, необходимые для применения команд 523
- объект пользовательского домена
 - ограничение 20
 - риск нарушения защиты 20
- объекта
 - (*Mgt), права доступа 138
 - (*Ref), права доступа 138
 - атрибут домена 16
 - атрибут режима 16
 - владелец по умолчанию (QDFTOWN), пользовательский профайл 152
 - восстановление 259, 263
 - выполнение (*EXECUTE), права доступа 138, 360
 - добавление (*ADD), права доступа 138, 360
 - защита с помощью списка прав доступа 176
 - измененный
 - поиск 322
 - обновление (*UPD), права доступа 138, 360
 - операционные права доступа (*OBJOPR) 138, 360
 - основная группа 127, 151
 - параметров контроля
 - изменение 93
 - по умолчанию 306
 - печать
 - источник прав доступа 754
 - предоставленные не фирмой IBM 754
 - принятые права доступа 754
 - пользовательский домен
 - ограничение 20
 - риск нарушения защиты 20
 - права доступа
 - *ALL (все) 140, 361
 - *CHANGE (изменение) 140, 361
 - *USE (использование) 140, 361
 - изменение 167
 - новый 147
 - новый объект 146
 - применение модельного 173
 - системное подмножество 140
 - хранение 261
 - часто используемое подмножество 140
 - права доступа, необходимые для выполнения команд 364
 - предоставленные не фирмой IBM
 - печать списка 334
 - принадлежность
 - введение 5
 - присвоение прав доступа и владельца 152
 - просмотр
 - инициатор 151
 - работа с 328
 - сбой неподдерживаемых интерфейсов 16
 - сохранение 259
 - существование (*OBJEXIST), права доступа 138, 360
 - удаление (*DLT), права доступа 138, 360
 - управление (*OBJMGT), права доступа 138, 360
 - управление доступом 16
 - хранение
 - права доступа 260, 261
- объекта (продолжение)
 - чтение (*READ), права доступа 138, 360
- объекты по основной группе
 - работа с 152
- обязательное вхождение в пароль цифр 57
- обязательное вхождение в пароль цифр (QPWDRQDDGT), системное значение 57
- обязательное изменение пароля (QPWDRQDDIF), системное значение 54
- ограничение
 - QSYSOPR (очередь сообщений системного оператора) 217
 - возможности 88
 - LMTCPB пользовательский профайл, параметр 88
 - изменение начального меню 87
 - изменение начальной программы 86
 - изменение программы обработки клавиши Attention 110
 - изменение текущей библиотеки 86, 221
 - разрешенные команды 88
 - разрешенные функции 88
 - список пользователей 320
- вход в систему
 - попытки (QMAXSGNACN), системное значение 33
 - попытки (QMAXSIGN), системное значение 32
- доступ
 - консоль 272
 - рабочие станции 272
- использование дисковой памяти (MAXSTG) 99
- использование системных ресурсов
 - ограничение приоритета (PTYLMT), параметр 100
 - командная строка, работа 88
 - команды (ALWLMTUSR) 88
 - операции восстановления 228
 - операции сохранения 228
 - повторяющиеся символы в пароле 56
 - последовательность цифр в пароле (системное значение QPWLMTAJC) 55
- сеансов одним устройством
 - LMTDEVSSN пользовательский профайл, параметр 98
 - параметров контроля 274
 - рекомендации 98
- сеансы устройства (QLMTDEVSSN), системное значение
 - вход в систему несколько устройств 31
 - описание 31
- символы в пароле 55
- системный администратор (QLMTSECOFR)
 - изменение уровня защиты 14
- системный администратор, системное значение (QLMTSECOFR) 272
 - вход в систему 213
 - описание 32

- ограничение (*продолжение*)
 - системный администратор, системное значение (QLMTSECOFR) (*продолжение*)
 - параметров контроля 272
 - права доступа к описаниям устройств 211
 - сообщения 21
 - число попыток входа в систему параметров контроля 272, 276
- ограничение приоритета (PTYLMT), параметр
 - пользовательский профайл 100
 - рекомендации 101
- ограничить возможности (LMTCPB), параметр
 - пользовательский профайл 88
- ограничить доступ для администратора защиты (QLMTSECOFR), системное значение
 - значение, устанавливаемое командой CFGSYSSECC 759
- ограничить срок действия пароля (PWDEXP), параметр 82
- операции с кластерами (CU), формат файла 622
- операции удаления (DO), формат файла 635
- Операционная поддержка, команды
 - права доступа к объектам, необходимые для применения команд 477
- операционная система
 - защита при установке 269
- операционные права доступа (*OBJOPR) 138, 360
- операция восстановления
 - максимальный объем памяти (MAXSTG) 99
 - необходимый объем памяти 99
- операция удаления (DO), тип записи журнала 288
- описание
 - защита меню 242
 - требования к защите библиотек 240
- описание (TEXT), параметр
 - пользовательский профайл 89
- Описание NetBIOS
 - права доступа к объектам, необходимые для применения команд 470
- описание NetBIOS (*NTBD), контроль 567
- описание задания (*JOBDD), контроль за объектом 557
- описание задания (JOBDD), параметр
 - пользовательский профайл 101
- описание запроса на изменение
 - права доступа к объектам, необходимые для применения команд 377
- описание запроса на изменение (*CRQD), контроль за объектом 534
- описание класса обслуживания (*COSD), контроль 537
- описание контроллера (*CTLD), контроль 538
- описание линии
 - права доступа к объектам, необходимые для применения команд 462
- описание линии (*LIND), контроль 561
- описание локали C (*CLD), контроль 534
- описание объекта
 - просмотр 328
- описание подсистемы
 - запись 334
 - защита 215
 - изменение записи маршрутизации запись журнала контроля (QAUDJRN) 299
 - печать параметров, влияющих на защиту 754
 - печать списка описаний 334
 - пользователь по умолчанию 334
 - права доступа 334
 - производительность 229
 - средства связи, запись 216
- описание подсистемы (*SBSD), контроль 577
- описание режима
 - права доступа к объектам, необходимые для применения команд 469
- описание режима (*MODD), контроль 563
- описание сеанса (*SSND), контроль 584
- описание сетевого сервера
 - права доступа к объектам, необходимые для применения команд 475
- описание сетевого сервера (*NWSD), контроль 568
- описание системы S/36 (*S36), контроль 587
- описание устройства
 - защита 211
 - определение 211
 - печать параметров, влияющих на защиту 754
 - права доступа к объектам, необходимые для применения команд 390
 - права на использование 211
 - принадлежность
 - изменение 213
 - по умолчанию, владелец 213
 - принадлежит профайлу QPGMR (программист) 213
 - принадлежит профайлу QSECOFR (системный администратор) 213
 - создание
 - QCRTAUT (права при создании), системное значение 146
 - общие права доступа 146
- описание устройства (*DEVDD), контроль 539
- описание формата
 - права доступа к объектам, необходимые для применения команд 403
- описание часового пояса, команды 518
- описанный в программе файл
 - сохранение прав доступа при удалении 160
- определение запроса (*QRYDFN), контроль 575
- определение продукта (*PRDDFN), контроль 573
- определение страницы (*PAGDFN), контроль 570
- определение формы (*FORMDF), контроль за объектом 554
- оптическая память
 - права доступа к объектам, необходимые для применения команд 478
- опции пользователя (CHRIDCTL), параметр
 - пользовательский профайл 112
- опции пользователя (SETJOBATR), параметр
 - пользовательский профайл 112
- опция пользователя (LOCALE), параметр
 - пользовательский профайл 113
- опция пользователя (USROPT), параметр
 - *CLKWD (ключевое слово CL) 112, 113, 114
 - *EXPERT (эксперт) 112, 113, 114, 167
 - *HLPFULL (полноэкранный справочник) 114
 - *NOSTMSG (сообщение об отсутствии состояния) 114
 - *PRTMSG (печать сообщения) 114
 - *ROLLKEY (клавиша прокрутки) 114
 - *STMSG (сообщение о состоянии) 114
 - пользовательский профайл 112, 113
- орфографический словарь
 - права доступа к объектам, необходимые для применения команд 507
- орфографический словарь (*SPADCT), контроль 580
- основная группа
 - введение 6
 - восстановление 259, 264
 - изменение 152
 - запись журнала контроля (QAUDJRN) 298
 - описание команды 328
 - изменение во время восстановления информации
 - запись журнала контроля (QAUDJRN) 293
 - изменение при восстановлении 264
 - новый объект 152
 - описание 151
 - определение 137
 - планирование 252
 - работа с 129, 172
 - работа с объектами 328
 - сохранение 259
 - удаление
 - профайл 127
- основная группа, права доступа
 - права доступа, пример проверки 196
- основной (*BASIC), уровень
 - поддержки 78, 85

- основной служебный пользовательский профайл (QSRVBAS)
 - значения по умолчанию 339
 - права доступа к консоли 213
- особые файлы (*CHRSF), контроль 533
- от имени
 - параметров контроля 562
- отклонение
 - iSeries Access, доступ 226
 - доступ
 - DDM, запрос (DDM) 227
 - удаленное задание, запуск 225
- отключен (*DISABLED), состояние пользовательского профайла
 - QSECOFR (пользовательский профайл системного администратора) 83
 - описание 83
- отключение
 - контроль, функция 313
 - получатель журнала 311
 - получатель журнала контроля 311, 312
 - пользовательский профайл 83
 - автоматически 749
 - уровень защиты 40 20
 - уровень защиты 50 22
- отладка, функции
 - принятые права доступа 158
- отмена
 - контроль, функция 313
- Отправить буферный файл по сети (SNDNETSPLF), команда 222
- Отправить запись журнала (SNDJRNE), команда 310
- отправка
 - запись журнала 310
 - сеть, буферный файл 222
- отслеживание
 - *ALLOBJ (ко всем объектам), специальные права доступа 274
 - IBM, поставляемые пользовательские профайлы 272
 - важные данные
 - права доступа 275
 - шифрование 277
 - вход в систему без ИД и пароля пользователя 276
 - группа, профайл
 - пароль 274
 - членство 274
 - использование
 - QHST (протокол хронологии) 318
 - журналы 318
 - очередь сообщений QSYSMSG 276
 - неподдерживаемые интерфейсы 277
 - неработающие пользователи 275
 - несанкционированный доступ 276
 - несанкционированный доступ к программам 277
 - обзор 271
 - ограничение возможностей 274
 - описания заданий 275
 - пользовательский профайл
 - администрирование 274
 - права доступа 275
 - пользовательских профайлов 275
 - права доступа к объектам 321
 - отслеживание (*продолжение*)
 - права доступа программиста 274
 - принятые права доступа 276
 - программный сбой 322
 - сетевые атрибуты 277
 - системный администратор 323
 - системных значений 272
 - сообщение
 - защита 317
 - списки библиотек 276
 - способы 317
 - справочная таблица 272
 - средства связи 277
 - средства управления паролями 273
 - удаленный вход в систему 277
 - физическая защита 272
 - целостность объекта 322
 - шифрование конфиденциальных данных 277
 - отсутствие необходимых прав доступа (AF), формат файла 604
 - очередь вывода
 - *JOBCTL (управление заданиями), специальные права доступа 91
 - *OPRCTL (управляется оператором), параметр 91
 - *SPLCTL (управление буфером), специальные права доступа 91
 - AUTCHK (права на исправление), параметр 223
 - DSPDTA (показать данные), параметр 222
 - OPRCTL (управляется оператором), параметр 223
 - защита 221, 224
 - изменение 222
 - печать параметров, влияющих на защиту 334, 756
 - показать данные (DSPDTA), параметр 222
 - пользовательский профайл 108
 - права доступа к объектам, необходимые для применения команд 481
 - права на исправление (AUTCHK), параметр 223
 - работа с описанием 222
 - создание 222, 224
 - управляется оператором (OPRCTL), параметр 223
 - очередь вывода (*OUTQ), контроль 568
 - очередь вывода (OUTQ), параметр пользовательский профайл 108
 - очередь данных
 - права доступа к объектам, необходимые для применения команд 390
 - очередь заданий
 - *JOBCTL (управление заданиями), специальные права доступа 91
 - *OPRCTL (управляется оператором), параметр 91
 - *SPLCTL (управление буфером), специальные права доступа 91
 - печать параметров, влияющих на защиту 334, 756
 - очередь заданий (*продолжение*)
 - права доступа к объектам, необходимые для применения команд 442
 - очередь заданий (*JOBQ), контроль 557
 - очередь сообщений (*MSGQ), контроль 565
 - очередь сообщений QSYSMSG
 - QMAXSGNACN (действие при достижении максимального числа попыток), системное значение 34
 - QMAXSIGN (максимальное число попыток входа в систему), системное значение 33
 - параметров контроля 276, 317
 - очередь сообщений неактивного задания (QINACTMSGQ), системное значение
 - значение, устанавливаемое командой CFGSYSSEC 759
 - очистка
 - права доступа к объектам, необходимые для применения команд 477
 - ошибка в сетевом пароле (VP), формат файла 725
 - ошибка прав доступа
 - вход в систему 209
 - задание, инициализация 209
 - запись журнала контроля (QAUDJRN) 292
 - запрещенная команда 19
 - нарушение аппаратной защиты 18
 - нарушение входа в систему по умолчанию 17
 - нарушение описания задания 17
 - неподдерживаемый интерфейс 17, 19
 - описание устройства 211
 - проверка программы 18, 19
 - ошибка прав доступа (*AUTFAIL), уровень контроля 286
 - ошибка сетевого пароля (VP), тип записи журнала 288

П

- пакет
 - права доступа к объектам, необходимые для применения команд 482
- пакет SQL (*SQLPKG), контроль 582
- пакетное задание
 - *SPLCTL (управление буфером), специальные права доступа 91
 - защита при запуске 209, 210
 - приоритет 100
- пакетный режим
 - ограничение заданий 229
- память
 - восстановление 21, 152, 269
 - QALWUSRDMN (разрешить пользовательские объекты), системное значение 28
 - максимальный (MAXSTG), параметр 99
 - пользовательский профайл 99

память *(продолжение)*
 пороговый объем
 контроль (QAUDJRN), получатель
 журнала 310
 расширенная аппаратная защита 18
 управление совместным
 использованием
 QSHRMEMCTL (управление общей
 памятью), системное
 значение 38
память, пул 229
папка
 защита общих 227
параметр
 проверка 18
параметр Начальная программа
(INLPGM)
 изменение 86
 пользовательский профайл 86
параметр Очередь сообщений (MSGQ)
 пользовательский профайл 106
параметр пользовательского профайла
 номер ИД группы, (GID) 114
параметр Текущая библиотека (CURLIB)
 пользовательский профайл 85
параметров контроля 308, 527
 *ALLOBJ (ко всем объектам),
 специальные права доступа 274
 *AUDIT (контроль), специальные права
 доступа 93
 IBM, поставляемые пользовательские
 профайлы 272
 аварийное завершение 69
 активация 308
 буферные файлы 581
 важные данные
 права доступа 275
 шифрование 277
 включение 308
 восстановление путей доступа 530
 вход в систему без ИД и пароля
 пользователя 276
 выключение 69
группа, профайл
 *ALLOBJ (ко всем объектам),
 специальные права доступа 274
 пароль 274
 членство 274
действия 278
завершение 69, 313
изменение
 описание команды 328, 331
использование
 QHST (протокол хронологии) 318
 журналы 318
 очередь сообщений QSYSMSG 276
настройка 308
неподдерживаемые интерфейсы 277
неработающие пользователи 275
несанкционированный доступ 276
несанкционированный доступ к
 программам 277
обзор 271
объекта
 планирование 304
 по умолчанию 306
объекты QTEMP 307

параметров контроля *(продолжение)*
 ограничение возможностей 274
 операции сохранения 270
 описания заданий 275
 ошибки 69
 планирование
 обзор 278
 системных значений 306
 пользовательский профайл
 *ALLOBJ (ко всем объектам),
 специальные права доступа 274
 администрирование 274
 почтовые службы 562
 права доступа 275
 пользовательских профайлов 275
 права доступа к объектам 321
 права доступа программиста 274
 принятые права доступа 276
 программный сбой 322
 процедура запуска 308
 работа от имени 562
 работа со средствами контроля
 пользователей 132
 Сервер каталогов 542
 сетевые атрибуты 277
 системный администратор 323
 системных значений 68, 272, 306
 службы Office 562
 списки библиотек 276
 список ответов 576
 способы 317
 справочная таблица 272
 средства связи 277
 средства управления паролями 273
 удаленный вход в систему 277
 управление 69
 физическая защита 272
 целостность объекта 322
 шифрование конфиденциальных
 данных 277
пароли
 уровни паролей 320
Пароли 52
пароль
 DST (специальные сервисные средства)
 изменение 135
 параметров контроля 273
 PWDEXP (ограничить срок действия
 пароля) 82
 QPGMR (профайл программиста) 761
 QSRV (служебный пользовательский
 профайл) 761
 QSRVBAS (основной служебный
 пользовательский профайл) 761
 QSYSOPR (профайл системного
 оператора) 761
 QUSER (профайл пользователя) 761
 возможные значения 81
 восстановление
 DST (специальные сервисные
 средства) 294
 пользователь 81
длина
 максимальная (QPWDMAXLEN),
 системное значение 54
 минимальная (QPWDMINLEN),
 системное значение 53

пароль *(продолжение)*
документ
 DOCPWD пользовательский
 профайл, параметр 106
запрет
 повторяющиеся символы 56
 последовательность цифр
 (системное значение
 QPWDLMTAJC) 55
 слова 55
 тривиальный 50, 273
запрет повторяющихся символов в
 пароле (QPWDLMTREP), системное
 значение
 значение, устанавливаемое
 командой CFGSYSSEC 759
запрет совпадения символов в
 одинаковых позициях в пароле
 (QPWDPOSDF), системное значение
 значение, устанавливаемое
 командой CFGSYSSEC 759
запрет цифр в соседних позициях в
 пароле (QPWDLMTAJC), системное
 значение
 значение, устанавливаемое
 командой CFGSYSSEC 759
изменение
 DST (специальные сервисные
 средства) 329
 описание 329
 применение пароля, системные
 значения 50
 указание пароля, совпадающего с
 именем пользователя 81
изменения при восстановлении
 профайла 262
команды 329
локальное управление паролем
 LCLPWDMGT пользовательский
 профайл, параметр 97
максимальная длина
 (QPWDMAXLEN), системное
 значение 54
максимальная длина пароля
 (QPWDMAXLEN), системное
 значение
 значение, устанавливаемое
 командой CFGSYSSEC 759
минимальная длина (системное
 значение QPWDMINLEN) 53
минимальная длина пароля
 (QPWDMINLEN), системное значение
 значение, устанавливаемое
 командой CFGSYSSEC 759
недопустимые для пароля символы
 (QPWDLMTCHR), системное
 значение
 значение, устанавливаемое
 командой CFGSYSSEC 759
немедленное истечение срока
 действия 51
ограничение
 повторяющиеся символы 56
 последовательность цифр
 (системное значение
 QPWDLMTAJC) 55
символы 55

- пароль (*продолжение*)
- ограничение срока действия, (PWDEXP) 82
 - ошибка
 - запись журнала контроля (QAUDJRN) 287
 - параметров контроля
 - DST (специальные сервисные средства) 273
 - пользователь 273
 - поиск 133, 329
 - пользовательский профайл 80
 - пользовательский профайл, поставляемый IBM
 - изменение 134
 - параметров контроля 272
 - потерянный 81
 - правила 81
 - предупреждение об истечении срока действия
 - QPWDEXPWRN, системное значение 52
 - проверка значений по умолчанию 749
 - проверка совпадения паролей (QPWDRQDDIF), системное значение, устанавливаемое командой CFGSYSSEC 759
 - программа выхода проверки
 - пример 65
 - программа подтверждения
 - QPWDLVDPGM, системное значение 63
 - защита, риск 64
 - пример 65
 - требования 64
 - программа проверки
 - QPWDLVDPGM, системное значение 63
 - защита, риск 64
 - пример 65
 - требования 64
 - программа проверки пароля (QPWDLVDPGM), системное значение
 - значение, устанавливаемое командой CFGSYSSEC 759
 - разрешение на изменение пользователями 273
 - рекомендации 81, 82
 - сеть
 - запись журнала контроля (QAUDJRN) 288
 - символы в одинаковых позициях (QPWDPOSIDF), системное значение 57
 - системный 137
 - системных значений
 - обзор 49
 - совпадает с именем пользовательского профайла 50, 81
 - состоящий только из цифр 80
 - средства связи 54
 - срок действия
 - PWDEXPITV пользовательский профайл, параметр 96
 - QPWDEXPITV, системное значение 51
- пароль (*продолжение*)
- срок действия (*продолжение*)
 - параметров контроля 273
 - срок действия истек (PWDEXP), параметр 82
 - срок действия пароля (QPWDEXPITV), системное значение
 - значение, устанавливаемое командой CFGSYSSEC 759
 - требование
 - изменение (системное значение QPWDRQDDIF) 54
 - изменить (параметр PWDEXPITV) 96
 - изменить (системное значение QPWDEXPITV) 51
 - полное изменение 57
 - цифра 57
 - требовать наличия цифр в пароле (QPWDRQDDGT), системное значение
 - значение, устанавливаемое командой CFGSYSSEC 759
 - тривиальный
 - запрет 50, 273
 - шифрование 81
 - пароль (PW), тип записи журнала 287
 - пароль процессора 137
 - пароль, проверка 63
 - пароль, состоящий только из цифр 80
 - Передать задание на выполнение (SBMJOB), команда 210
 - SECBATCH, меню 752
 - Передать управление (TFRCTL), команда
 - передача принятых прав доступа 157
 - передача на обработку
 - отчеты о защите 752
 - переименование
 - объекта
 - запись журнала контроля (QAUDJRN) 291
 - пользовательский профайл 131
 - Перейти к групповому заданию (TFRGRPJOB), команда
 - принятые права доступа 158
 - перекрытие (*OVL), контроль 570
 - перемещение
 - к групповому заданию 158
 - принятые права доступа 157, 158
 - перенос
 - буферный файл 222
 - объекта
 - запись журнала контроля (QAUDJRN) 291
 - права доступа к объектам, необходимые для применения команд 468
 - уровень защиты (QSECURITY), системное значение
 - с уровня 10 на уровень 20 13
 - с уровня 20 на уровень 30 13
 - с уровня 20 на уровень 40 19
 - с уровня 20 на уровень 50 22
 - с уровня 30 на уровень 20 13
 - с уровня 30 на уровень 40 19
 - с уровня 30 на уровень 50 22
 - с уровня 40 на 20 13
- переопределение, команды 251
- печатаемый вывод (*PRTDTA), уровень контроля 293
- Печатать атрибуты защиты системы (PRTSYSSECA), команда
 - описание 335, 754
- Печатать права доступа к описанию подсистемы (PRTSBSDAUT), команда
 - описание 334
- Печатать права доступа к описаниям заданий (PRTJOBDAUT), команда
 - описание 754
- Печатать права доступа к очереди (PRTQAUT), команда
 - описание 334, 756
- Печатать принимающие объекты (PRTADPOBJ), команда
 - описание 754
- печать 114
 - владелец прав доступа 334
 - записи журнала контроля 754
 - запись журнала контроля (QAUDJRN) 293
 - защита 221
 - значения описания подсистемы, влияющие на защиту 754
 - информация о принимающем объекте 754
 - информация о списке прав доступа 754
 - объекты с общими правами доступа 756
 - отправка сообщения (*PRTMSG, опция пользователя) 114
 - параметры очереди вывода, влияющие на защиту 334, 756
 - параметры очереди заданий, влияющие на защиту 334, 756
 - параметры связи, влияющие на защиту 754
 - программы триггеров 334, 754
 - сетевые атрибуты 335, 754
 - системных значений 272, 335, 754
 - список объектов, предоставленных не фирмой IBM 334, 754
 - список описаний подсистем 334
 - средства связи 335
 - уведомление (*PRTMSG, опция пользователя) 114
- Печать объектов с общими правами доступа (PRTPUBAUT), команда
 - описание 756
- Печать описания подсистемы (PRTSBSDAUT), команда
 - описание 754
- Печать параметров защиты средств связи (PRTCMNSEC), команда
 - описание 335, 754
- Печать пользовательских объектов (PRTUSROBJ), команда
 - описание 334, 754
- Печать пользовательского профайла (PRTUSRPRF), команда
 - описание 754
- Печать программ триггеров (PRTTRGPGM), команда
 - описание 334, 754

печать сообщения (*PRMSG), опция пользователя 114
 Печать частных прав доступа (PRTPVTAUT), команда 334
 описание 756
 список прав доступа 754
 планирование
 библиотека, разработка 236
 защита 1
 защита для системных программистов 256
 защита команд 248
 защита меню 240
 защита файлов 248
 контроль
 системных значений 306
 несколько групп 252
 основная группа 252
 отчеты о защите 753
 параметров контроля
 действия 278
 обзор 278
 объекты 304
 пользовательский профайл
 активация 749
 истечение срока хранения 749
 программист, защита 254
 профайлы групп 251
 справочная таблица 272
 средства управления паролями 273
 физическая защита 272
 планирование изменения уровня пароля QPWDVLV, изменение 233
 изменение уровня паролей (с 0 до 1) 233
 изменение уровня паролей (с 2 на 3) 235
 изменение уровня паролей с 1 на 0 236
 изменение уровня паролей с 2 на 0 236
 изменение уровня паролей с 2 на 1 235
 изменение уровня паролей с 3 на 0 235
 изменение уровня паролей с 3 на 1 235
 изменение уровня паролей с 3 на 2 235
 изменение уровня пароля
 планирование изменения уровня 233
 повышение уровня паролей 233
 снижение уровня паролей 235, 236
 планировщик заданий (*JOBSCD), контроль за объектом 558
 по умолчанию 339
 *DFT, режим доставки
 пользовательский профайл 107
 владелец (QDFTOWN)
 восстановление программ 267
 запись журнала контроля (QAUDJRN) 293
 значения по умолчанию 339
 описание 152
 вход в систему
 описание подсистемы 215
 по умолчанию (*продолжение*)
 вход в систему (*продолжение*)
 уровень защиты 40 17
 значение
 пользовательский профайл 337
 пользовательский профайл, поставляемый IBM 337
 объекта
 параметров контроля 306
 описание задания (QDFTJOB) 101
 поврежденный журнал контроля 310
 поврежденный список прав доступа
 восстановление 268
 поддержка печати по TCP/IP (QTMPLPD),
 пользовательский профайл 339
 подмножество
 права доступа 140
 подсистема
 *JOBCTL (управление заданиями),
 специальные права доступа 91
 вход в систему без ИД пользователя и
 пароля 17
 права доступа к объектам,
 необходимые для применения
 команд 510
 подтверждение, пароль 63
 поиск 177
 изменения объектов 277, 322, 330
 измененные объекты 322
 пароли по умолчанию 749
 пароль 133, 329
 целостность объекта 754
 контроль использования 277
 описание 322, 330
 Показать библиотеку (DSPLIB),
 команда 321
 Показать буферный файл (DSPSPLF),
 команда 222
 Показать владельца прав доступа
 (DSPAUTHLR), команда 160, 327
 Показать журнал (DSPJRN), команда
 контроль операций с файлами 248,
 319
 пример журнала контроля
 (QAUDJRN) 313, 314
 просмотр QAUDJRN (журнала
 контроля) 278
 создание файла вывода 315
 Показать записи журнала контроля
 (DSPAUDJRNE), команда
 описание 334, 754
 Показать записи таблицы ключей Kerberos
 (DSPKRBKTE), команда
 необходимые права доступа к
 объектам 449
 показать информацию о входе в систему
 (QDSPSGNINF), системное значение
 значение, устанавливаемое командой
 CFGSYSSEC 759
 Показать объекты библиотеки документов
 списка прав доступа (DSPAUTLDLO),
 команда 332
 Показать объекты списка прав доступа
 (DSPAUTLJOB), команда 176, 327
 Показать описание библиотеки
 (DSPLIBD), команда
 CRTAUT, параметр 165
 Показать описание задания (DSPJOB),
 команда 276
 Показать параметры контроля действий
 (DSPSECAUD), команда
 описание 751
 Показать параметры контроля за
 действиями (DSPSECAUD), команда
 описание 334
 Показать параметры контроля объекта
 библиотеки документов (DSPDLOAUD),
 команда 332
 использование 306
 Показать пользователей с правами
 доступа (DSPAUTUSR), команда
 описание 330
 параметров контроля 320
 пример 130
 Показать пользователей с правами
 доступа (DSPAUTUSR), меню 130, 320
 Показать пользовательский профайл
 (DSPUSRPRF), команда
 использование 130
 описание 330
 с помощью файла вывода 320
 Показать права доступа (DSPAUT),
 команда 328
 Показать права доступа к объекту
 отображение сведений (*EXPERT,
 опция пользователя) 112, 113, 114
 пример 165, 166
 Показать права доступа к объекту
 (DSPOBJAUT), команда 321, 328
 Показать права доступа к объекту
 библиотеки документов (DSPDLOAUT),
 команда 332
 Показать принимающие программы
 (DSPPGMADP), команда
 использование 159, 248
 описание 331
 параметров контроля 322
 Показать программу (DSPPGM), команда
 принятые права доступа 159
 режим программы 16
 Показать расписание активации
 (DSPACTSCD), команда
 описание 749
 Показать расписание истечения срока
 (DSPEXPSCD), команда
 описание 749
 Показать служебную программу
 (DSPSRVPGM), команда
 принятые права доступа 159
 Показать список прав доступа (DSPAUTL),
 команда 327
 Показать файл кэша идентификационных
 данных Kerberos (DSPKRBCCF), команда
 необходимые права доступа к
 объектам 449
 поле, права доступа 142
 определение 138
 полное изменение пароля 57
 полное имя
 просмотр 172
 полномочия
 определение 137
 полноэкранный справочник (*HLPFULL),
 опция пользователя 114

полный
 контроль (QAUDJRN), получатель
 журнала 310
 получатель
 изменение 312
 отключение 311, 312
 сохранение 312
 удаление 312
 получатель журнала
 изменение 312
 максимальный объем памяти
 (MAXSTG) 99
 необходимый объем памяти 99
 отключение 311, 312
 права доступа к объектам,
 необходимые для применения
 команд 447
 удаление 312
 управление 311
 получатель журнала (*JRNRCV),
 контроль 560
 получатель журнала контроля
 присвоение имени 309
 создание 309
 сохранение 312
 удаление 312
 Получить запись списка прав доступа
 (RTVAUTLE), команда 327
 Получить информацию о получателе
 журнала, API
 контроля объекта 560
 Получить пользовательский профайл
 (RTVUSRPRF), команда 133, 330
 пользователь
 добавление 123
 параметров контроля
 изменение 93
 работа с 132
 регистрация 123
 пользователь (*USER), домен 16
 пользователь (*USER), режим 16
 пользователь Internet
 контрольные списки 256
 пользователь рабочей станции (QUSER),
 пользовательский профайл 339
 пользователь с правами доступа
 просмотр 330
 пользователь, права доступа
 аннулирование 332
 права доступа к объектам,
 необходимые для применения
 команд 476
 предоставление 332
 пользовательская очередь (*USRQ),
 контроль 590
 пользовательская очередь (*USRQ),
 объект 20
 пользовательская часть
 список библиотек
 описание 218
 рекомендации 221
 управление 238
 пользовательские права доступа (USER
 DEF) 167
 пользовательские профайлы,
 поставляемые IBM, с правами
 доступа 350, 358
 пользовательский индекс (*USRIDX),
 контроль 588
 пользовательский индекс (*USRIDX),
 объект 20
 пользовательский профайл
 (GID), номер ID группы 114
 *ALLOBJ (ко всем объектам),
 специальные права доступа 90
 *AUDIT (контроль), специальные права
 доступа 93
 *IOSYSCFG (конфигурация системы),
 специальные права доступа 94
 *JOBCTL (управление заданиями),
 специальные права доступа 91
 *SAVSYS (специальные права на
 сохранение системы) 92
 *SECADM (администратор защиты),
 специальные права доступа 90
 *SERVICE, специальные служебные
 права доступа 92
 *SPLCTL (управление буфером),
 специальные права доступа 91
 ACGCDE (код учета ресурсов) 105
 ASTLVL (уровень поддержки) 84
 ATNPGM (программа обработки
 клавиши Attention) 109
 AUDLVL (контроль действий) 118
 AUDLVL (уровень контроля)
 *CMD (текст команды),
 значение 288
 AUT (права доступа) 117
 CCSID (идентификатор набора
 символов) 111
 CNTRYID (идентификатор страны или
 региона) 111
 CURLIB (текущая библиотека) 85
 DEV (принтер) 108
 DLVRY (доставка в очередь
 сообщений) 107
 DOCPWD (пароль документа) 106
 DSPSGNINF (информация о входе в
 систему) 96
 EIMASSOC (связь eim) 115
 GRPAUT (права доступа группы) 103,
 150, 152
 GRPAUTTYP (тип прав доступа
 группы) 104, 152
 GRPPRF (профайл группы) 152
 изменения при восстановлении
 профайла 262
 описание 102
 HOMEDIR (домашний каталог) 115
 INLMNU (начальное меню) 87
 INLPGM (начальная программа) 86
 JOBID (описание задания) 101
 KBDBUF (буферизация
 клавиатуры) 98
 LANGID (идентификатор языка) 111
 LCLPWDGMT (локальное управление
 паролем) 97
 LMTCPB (ограничить
 возможности) 88, 221
 LMTDEVSSN (ограничить сеансы
 одним устройством) 98
 LOCALE (локаль) 113
 LOCALE (опции пользователя) 113
 пользовательский профайл (продолжение)
 MAXSTG (максимальный объем
 памяти)
 группа, принадлежность
 объектов 150
 описание 99
 MSGQ (очередь сообщений) 106
 OBJAUD (контроль за объектом) 117
 OUTQ (очередь вывода) 108
 OWNER (владелец создаваемых
 объектов) 103, 150
 OWNER (владелец) 152
 PTYLMT (ограничение
 приоритета) 100
 PWDEXP (ограничить срок действия
 пароля) 82
 PWDEXPITV (срок действия
 пароля) 96
 SEV (серьезность очереди
 сообщений) 108
 SPCAUT (специальные права
 доступа) 89
 SPCENV (специальная среда) 94
 SRTSEQ (последовательность
 сортировки) 110
 SUPGRPPRF (дополнительные
 группы) 105
 user identification number 114
 USRCLS (класс пользователя) 83
 USROPT (опции пользователя) 112,
 113
 USRPRF (имя) 79
 автоматическое создание 77
 администратор защиты (*SECADM),
 специальные права доступа 90
 анализ
 по классу пользователя 754
 по специальным правам
 доступа 754
 анализ с помощью запроса 320
 большой, проверка 321
 буферизация клавиатуры
 (KBDBUF) 98
 введение 4
 владелец (OWNER) 152
 владелец создаваемых объектов
 (OWNER) 103, 150
 восстановление
 запись журнала контроля
 (QAUDJRN) 294
 команды 259
 описание команды 331
 процедуры 262
 восстановление прав доступа
 запись журнала контроля
 (QAUDJRN) 293
 группа, профайл (GRPPRF) 152
 изменения при восстановлении
 профайла 262
 описание 102
 домашний каталог (HOMEDIR) 115
 дополнительные группы
 (SUPGRPPRF) 105
 доставка (DLVRY) 107
 доставка в очередь сообщений
 (DLVRY) 107
 загрузка 133, 330

- пользовательский профайл (*продолжение*)
- задать атрибут задания (опции пользователя) 112
 - ИД пользователя из цифр 79
 - идентификатор набора символов (CCSID) 111
 - идентификатор страны или региона (CNTRYID) 111
 - идентификатор языка (LANGID) 111
 - изменение
 - запись журнала контроля (QAUDJRN) 294
 - описания команд 330
 - пароль 329
 - состав пароля, системные значения 50
 - способы 127
 - указание пароля, совпадающего с именем пользователя 81
 - изменение при восстановлении 262
 - имя (USRPRF) 79
 - информация о принадлежности объекта 120
 - класс пользователя (USRCLS) 83
 - код учета ресурсов (ACGCDE) 105
 - команды 330
 - контроль (*AUDIT), специальные права доступа 93
 - контроль действий (AUDLVL) 118
 - контроль за объектом (OBJAUD) 117
 - Конфигурация системы (*IOSYSCFG), особые права доступа 94
 - копирование 124
 - локальное управление паролем (LCLPDMGT) 97
 - максимальный объем памяти (MAXSTG)
 - группа, принадлежность объектов 150
 - описание 99
 - начальная программа (INLPGM) 86
 - начальное меню (INLMNU) 87
 - номер ИД группы, (GID) 114
 - общие права доступа (AUT) 117
 - объект, владелец
 - удаление 150
 - ограничение возможностей
 - описание 88
 - параметров контроля 274
 - список библиотек 221
 - ограничение приоритета (PTYLMT) 100
 - ограничить сеансы одним устройством (LMTDEVSSN) 98
 - ограничить срок действия пароля (PWDEXP) 82
 - описание (TEXT) 89
 - описание задания (JOBID) 101
 - опции пользователя (CHRIDCTL) 112
 - опции пользователя (LOCALE) 113
 - опции пользователя
 - (SETJOBATR) 112
 - опции пользователя (USROPT) 112, 113
 - основная группа 129
 - очередь вывода (OUTQ) 108
 - очередь сообщений (MSGQ) 106
- пользовательский профайл (*продолжение*)
- параметров контроля
 - *ALLOBJ, специальные права доступа 274
 - пользователи с правами доступа 320
 - права на использование 275
 - пароль 80
 - пароль документа (DOCPWD) 106
 - переименование 131
 - печать 320
 - полный список 130
 - последовательность сортировки (SRTSEQ) 110
 - поставляемый IBM
 - параметров контроля 272
 - таблица значений по умолчанию 337
 - цель 134
 - права доступа
 - хранение 262
 - права доступа (AUT) 117
 - права доступа группы (GRPAUT) 103, 150, 152
 - права доступа к объектам, необходимые для применения команд 518, 520
 - применяемый в описании задания 17
 - принтер (DEV) 108
 - присвоение имени 80
 - проверка паролей по умолчанию 749
 - программа обработки клавиши Attention (ATNPGM) 109
 - производительность
 - сохранение и восстановление 120
 - просмотр
 - информация о входе в систему (DSPSGNINF) 96
 - описание команды 330
 - отдельный 130
 - принимающие программы 159
 - работа с 122, 330
 - разрешение применения
 - пример программы 130
 - роли 77
 - связанные команды 331
 - связь eim (EIMASSOC) 115
 - серьезность (SEV) 108
 - серьезность очереди сообщений (SEV) 108
 - служебные права доступа (*SERVICE) 92
 - создание
 - запись журнала контроля (QAUDJRN) 294
 - описание примера 123
 - описания команд 329, 330
 - способы 122
 - состояние (STATUS) 83
 - сохранение 259
 - сохранение системы (*SAVSYS), специальные права доступа 92
 - специальная среда (SPCENV) 94
 - специальные права доступа (SPCAUT) 89
 - специальные права доступа ко всем объектам (*ALLOBJ) 90
- пользовательский профайл (*продолжение*)
- список
 - все пользователи 130
 - выбранные 320
 - неактивный 320
 - пользователи с правами на выполнение команд 320
 - пользователи со специальными правами доступа 320
 - список постоянно активных
 - изменение 749
 - среда System/36 94
 - срок действия пароля (PWDEXPITV) 96
 - таблица значений по умолчанию 337
 - текст (TEXT) 89
 - текущая библиотека (CURLIB) 85
 - тип прав доступа группы (GRPAUTTYP) 104, 152
 - типы меню 131
 - типы отчетов 131
 - точки выхода 133
 - удаление
 - буферные файлы 129
 - запись каталога 127
 - описание команды 330
 - сообщения, очередь 127
 - списки рассылки 127
 - управление буфером (*SPLCTL), специальные права доступа 91
 - управление заданиями (*JOBCTL), специальные права доступа 91
 - уровень контроля (AUDLVL)
 - *CMD (текст команды), значение 288
 - уровень поддержки (ASTLVL) 84
 - хранение
 - права доступа 260, 262
 - частные права доступа 120
 - пользовательский профайл (*USRPRF), контроль 589
 - пользовательский профайл системного администратора (QSECOFR)
 - восстановление 263
 - значения по умолчанию 339
 - описание устройства, владелец 213
 - отключен, состояние 83
 - права доступа к консоли 213
 - разрешение применения 83
 - пользовательский профайл, поставляемый IBM
 - ADSM (QADSM) 339
 - AFDFTUSR (QAFDFTUSR) 339
 - AFOWN (QAFOWN) 339
 - AFUSR (QAFUSR) 339
 - BRM (QBRMS) 339
 - BRM, пользовательский профайл QBRMS 339
 - DCEADM (QDCEADM) 339
 - IBM, профайл прав доступа QAUTPROF 339
 - NFS, пользовательский профайл (QNFSANON) 339
 - QADSM (ADSM) 339
 - QAFDFTUSR (AFDFTUSR) 339
 - QAFOWN (AFOWN) 339
 - QAFUSR (AFUSR) 339

пользовательский профайл, поставляемый IBM (*продолжение*)

- QAUTPROF (общие базы данных) 339
- QAUTPROF (профайл прав доступа IBM) 339
- QBRMS (BRM) 339
- QBRMS (пользовательский профайл BRM) 339
- QDBSHR (общая база данных) 339
- QDCEADM (DCEADM) 339
- QDFTOWN (владелец по умолчанию) значения по умолчанию 339 описание 152
- QDOC (документ) 339
- QDSNX (узловой исполнитель в распределенных системах) 339
- QFNC (финансы) 339
- QGATE (мост VM/MVS) 339
- QLPAUTO (автоматическая установка лицензионной программы) 339
- QLPINSTALL (установка лицензионных программ) 339
- QMSF (среда почтового сервера) 339
- QNFSANON (пользовательский профайл NFS) 339
- QPGMR (программист) 339
- QRJE (запись удаленного задания) 339
- QSECOFR (системный администратор) 339
- QSNADS (службы рассылки системной сетевой архитектуры) 339
- QSPL (буфер) 339
- QSPLJOB (буферное задание) 339
- QSRV (служба) 339
- QSRVBAS (базовый профайл обслуживания) 339
- QSYS (система) 339
- QSYSOPR (системный оператор) 339
- QTCP (TCP/IP) 339
- QTMPLPD (поддержка печати по TCP/IP) 339
- QTSTRQS (тестовый запрос) 339
- QUSER (пользователь рабочей станции) 339
- TCP/IP (QTCP) 339
- автоматическая установка (QLPAUTO) 339
- базовый профайл обслуживания (QSRVBAS) 339
- буфер (QSPL) 339
- буферное задание (QSPLJOB) 339
- владелец по умолчанию (QDFTOWN) значения по умолчанию 339 описание 152
- восстановление 263
- документ (QDOC) 339
- запись удаленного задания (QRJE) 339
- изменение пароля 134
- команды с ограниченным доступом 347
- мост VM/MVS (QGATE) 339
- общая база данных (QDBSHR) 339
- параметров контроля 272
- поддержка печати по TCP/IP (QTMPLPD) 339

пользовательский профайл, поставляемый IBM (*продолжение*)

- пользователь рабочей станции (QUSER) 339
- права доступа, профайл QAUTPROF 339
- программист (QPGMR) 339
- система (QSYS) 339
- системный администратор (QSECOFR) 339
- системный оператор (QSYSOPR) 339
- служба (QSRV) 339
- службы рассылки SNA (QSNADS) 339
- среда почтового сервера (QMSF) 339
- таблица значений по умолчанию 337
- тестовый запрос (QTSTRQS) 339
- узловой исполнитель в распределенных системах (QDSNX) 339
- установка лицензионных программ (QLPINSTALL) 339
- финансы (QFNC) 339
- цель 134
- пользовательское пространство (*USRSPC), контроль 590
- пользовательское пространство (*USRSPC), объект 20
- последовательность сортировки QSRTSEQ, системное значение 110
- общий вес 110
- пользовательский профайл 110
- уникальный вес 110
- поточковый файл (*STMF), контроль 584
- почта
 - обработка
 - запись журнала контроля (QAUDJRN) 291
 - почтовые службы
 - действие, контроль 562
- права доступа 177
 - *ADD (добавление) 138, 360
 - *ALL (все) 140, 361
 - *ALLOBJ (ко всем объектам), специальные права доступа 90
 - *AUDIT (контроль), специальные права доступа 93
 - *AUTLMGT (управление списком прав доступа) 138, 145, 360
 - *CHANGE (изменение) 140, 361
 - *DLT (удаление) 138, 360
 - *EXCLUDE (запретить) 140
 - *EXECUTE (выполнение) 138, 360
 - *IOSYSCFG (конфигурация системы), специальные права доступа 94
 - *JOBCTL (управление заданиями), специальные права доступа 91
 - *Mgt 138
 - *OBJALTER (изменение объекта) 138, 360
 - *OBJEXIST (существование объекта) 138, 360
 - *OBJMGT (управление объектом) 138, 360
 - *OBJOPR (операционные права доступа к объекту) 138, 360
 - *OBJREF (обращение к объекту) 138, 360
 - *R (чтение) 140, 362

права доступа (*продолжение*)

- *READ (чтение) 138, 360
- *Ref (обращение) 138
- *RW (чтение, запись) 140, 362
- *RWX (чтение, запись, выполнение) 140, 362
- *RX (чтение, выполнение) 140, 362
- *SAVSYS (специальные права на сохранение системы) 92
- *SECADM (администратор защиты), специальные права доступа 90
- *SERVICE, специальные служебные права доступа 92
- *SPLCTL (управление буфером), специальные права доступа 91
- *UPD (обновление) 138, 360
- *USE (использование) 140, 361
- *W (запись) 140, 362
- *WX (запись, выполнение) 140, 362
- *X (выполнение) 140, 362
- библиотека 6
- введение 5
- восстановление
 - запись журнала контроля (QAUDJRN) 293
 - обзор команд 259
 - описание команды 331
 - описание процесса 266
 - процедура 265
- группа
 - пример 196, 200
 - просмотр 163
- данные
 - определение 138
 - добавление пользователей 168
 - игнорирование принятых 160
 - изменение 612
 - запись журнала контроля (QAUDJRN) 297
 - описание команды 328
 - процедуры 167
- изменение объекта (*OBJALTER) 138, 360
- каталог 6
- копирование
 - описание команды 330
 - переименование профайла 132
 - пример 127
 - рекомендации 173
- меню 162
- модельный объект
 - использование 173
- несколько объектов 169
- новый объект
 - CRTAUT (права при создании), параметр 146, 165
 - GRPAUT (права доступа группы), параметр 103, 150
 - GRPAUTTYP (тип прав доступа группы), параметр 104
 - QCRTAUT (права при создании), системное значение 28
 - QUSEADPAUT (Применять принятые права доступа), системное значение 38
 - пример 152

- права доступа (*продолжение*)
- обращение к объекту (*OBJREF) 138, 360
 - общие
 - восстановление 259, 264
 - определение 137
 - пример 198, 201
 - сохранение 259
 - объекта
 - *ADD (добавление) 138, 360
 - *DLT (удаление) 138, 360
 - *EXECUTE (выполнение) 138, 360
 - *OBJEXIST (существование объекта) 138, 360
 - *OBJMGT (управление объектом) 138, 360
 - *OBJOPR (операционные права доступа к объекту) 138, 360
 - *READ (чтение) 138, 360
 - *Ref (обращение) 138
 - *UPD (обновление) 138, 360
 - запретить (*EXCLUDE) 140
 - определение 138
 - формат хранения на носителе 261
 - хранение 260
 - хранение на носителе 261
 - определение 138
 - основная группа 137, 151
 - пример 196
 - работа с 129
 - отображение сведений (*EXPERT, опция пользователя) 112, 113, 114
 - параметров контроля 275
 - поиск 177
 - вход в систему 209
 - интерактивное задание, инициализация 209
 - пакетное задание, инициализация 210
 - поле
 - определение 138
 - пользовательские 167
 - пользовательский профайл
 - формат хранения на носителе 262
 - хранение 260
 - хранение на носителе 262
 - права на изменение 167
 - предоставление прав доступа по шаблону 169
 - принятые 611
 - запись журнала контроля (QAUDJRN) 292
 - игнорирование 245
 - параметров контроля 322
 - права доступа, пример проверки 199, 201
 - приложение, разработка 242, 245, 246
 - просмотр 163, 248
 - цель 156
 - присвоение новым объектам 152
 - просмотр
 - описание команды 328
 - работа с
 - описание команды 328
 - сведения, отображение (*EXPERT, опция пользователя) 112, 113, 114
- права доступа (*продолжение*)
- системное подмножество 140
 - сохранение при удалении файла 160
 - специальные права доступа (SPCAUT), параметр 89
 - список прав доступа
 - управление (*AUTLMGT) 138, 360
 - формат хранения на носителе 261
 - хранение 261
 - хранение на носителе 261
 - удаление пользователя 169
 - управление, права доступа
 - *Mgt(*) 138
 - хранение
 - с объектом 260
 - с пользовательским профайлом 260
 - список прав доступа 261
 - частные
 - восстановление 259, 264
 - определение 137
 - сохранение 259
 - часто используемое подмножество 140
 - права доступа (AUT), параметр
 - настройка списка прав доступа (*AUTL) 174
 - пользовательский профайл 117
 - создание библиотек 165
 - создание объектов 166
- права доступа к объектам
- *ALLOBJ (ко всем объектам), специальные права доступа 90
 - *SAVSYS (специальные права на сохранение системы) 92
 - Advanced Function Printing, команды 372
 - AF_INET, сокет для SNA 373
 - DNS, команды 401
 - NetBIOS, команды описания 470
 - PTF (временное исправление программы), команды 502
 - Query Management/400, команды 494
 - RJE (запись удаленного задания), команды 498
 - TCP/IP, команды 516
 - Token-Ring, команды 464
 - анализ 321
 - аннулирование 328
 - аппаратное обеспечение, команды 497
 - атрибуты защиты, команды 502
 - библиотека, команды 456
 - буферный файл, команды 508
 - владелец прав доступа, команды 375
 - вопросы и ответы, команды 495
 - восстановление путей доступа 371
 - временное исправление команды (PTF), команды 502
 - вывод на принтер, команды 508
 - графические операции 412
 - группа панелей, команды 465
 - двухбайтовая кодировка, команды 402
 - диалоговое обучение, команды 476
 - документ, команды 396
 - журнал, команды 443
 - загрузчик принтера, команды 524
- права доступа к объектам (*продолжение*)
- загрузчик, команды 524
 - задание, команды 437
 - изменение
 - запись журнала контроля (QAUDJRN) 297
 - процедуры 167
 - индекс поиска информации, команды 436
 - интерактивное определение данных 435
 - информация о заказе на обновление, команды 518
 - исходная информация связи, команды 383
 - к командам *CMD 382
 - каталог реляционной базы данных, команды 497
 - каталог связывания 376
 - каталог, команды 393
 - классы, команды 377
 - код доступа, команды 476
 - команды 328
 - Команды для работы с DNS 401
 - Команды для работы с Kerberos 448
 - команды для работы с сервером каталогов 394
 - контроль за действиями, команды 502
 - контрольный список 523
 - конфигурация сетевого сервера, команды 475
 - конфигурация, команды 384
 - лицензионная программа, команды 461
 - локаль, команды 464
 - меню, команды 465
 - набор графических символов, команды 413
 - неполадка, команды 489
 - носитель, команды 464
 - область данных, команды 389
 - общие команды работы с объектами 364
 - объект библиотеки документов (DLO), команды 396
 - объект настройки рабочей станции, команды 523
 - Операционная поддержка, команды 477
 - описание задания, команды 441
 - описание запроса на изменение, команды 377
 - описание класса обслуживания, команды 378
 - описание контроллера, команды 386
 - описание линии, команды 462
 - описание предупреждения, команды 373
 - описание режима, команды 469
 - описание сетевого интерфейса, команды 473
 - описание сетевого сервера, команды 475
 - описание сообщения, команды 467
 - описание устройства, команды 390
 - описание формата, команды 403

- права доступа к объектам *(продолжение)*
 - определение 138
 - оптическая память, команды 478
 - орфографический словарь, команды 507
 - отображение сведений (*EXPERT, опция пользователя) 112, 113, 114
 - очередь вывода, команды 481
 - очередь данных, команды 390
 - очередь заданий, команды 442
 - очередь сообщений, команды 468
 - очистка, команды 477
 - пакет, команды 482
 - перенос данных, команды 468
 - подсистема, команды 510
 - поиск, команды для работы с индексом 436
 - получатель журнала, команды 447
 - пользовательские индексы, очередь и пространство, команды 518
 - пользовательский профайл, команды 518, 520
 - права доступа пользователя, команды 476
 - предоставление 328
 - влияние на существующие права доступа 170
 - несколько объектов 169
 - предупреждение, команды 373
 - программа чтения, команды 496
 - программа, команды 490
 - программирование, команды для работы с языками 450
 - просмотр 321, 328
 - расписание заданий, команды 443
 - рассылка, команды 395
 - расширенная беспроводная локальная сеть, команды настройки 403
 - редактирование 167, 328
 - резервное копирование, команды 477
 - ресурс, команды 497
 - сведения, отображение (*EXPERT, опция пользователя) 112, 113, 114
 - сеанс, команды 498
 - сервер хоста 413
 - сервер, идентификация 502
 - сетевой атрибут, команды 471
 - сетевой сервер, команда 473
 - системное значение, команды 513
 - системные команды 512
 - системный список ответов, команды 513
 - служебные команды 502
 - список конфигурации, команды 385
 - список ответов, команды 513
 - список прав доступа, команды 375
 - список рассылки, команды 396
 - список соединений, команды 385
 - список узлов, команды 475
 - среда System/36, команды 513
 - среда почтового сервера, команды 464
 - статистика, команды 482
 - сфера управления, команды 507
 - таблица предупреждений, команды 373
- права доступа к объектам *(продолжение)*
 - таблица управления формами, команда 498
 - таблица, команды 516
 - текстовый индекс, команды 476
 - удаленный вход в систему дисплейной станции, команды 394
 - управление фиксацией, команды 383
 - файл сообщений, команды 468
 - файл, команды 404
 - фильтр, команды 411
 - финансовые команды 412
 - формат диаграммы, команды 377
 - формат хранения на носителе 261
 - хранение 260, 261
 - шифрование, команды 388
 - эмуляция, команды 392
 - языки программирования, команды 450
 - права доступа к полю 142
 - права доступа пользователя
 - добавление 168
 - копирование
 - описание команды 330
 - переименование профайла 132
 - пример 127
 - рекомендации 173
 - права доступа, кэш
 - частные права доступа 207
 - права доступа, объединение, специальные 253
 - права доступа, объект 321
 - права доступа, пользовательский профайл (QAUTPROF) 339
 - права доступа, проверка 177
 - владелец, права доступа
 - блок-схема 184
 - группа, права доступа
 - пример 196, 200
 - общие права доступа
 - блок-схема 190
 - пример 198, 201
 - основная группа
 - пример 196
 - порядок 177
 - принятые права доступа
 - блок-схема 191
 - пример 199, 201
 - список прав доступа
 - пример 202
 - частные права доступа
 - блок-схема 182
 - права доступа, специальные 253
 - права доступа, типы
 - сочетание
 - пример 204
 - права на выполнение команд
 - список пользователей 320
 - права при создании (CRTAUT), параметр
 - описание 146
 - просмотр 165
 - риски 146
 - права при создании (QCRTAUT), системное значение
 - использование 146
 - описание 28
 - риск изменения 28
- превышение
 - максимальное число учетных записей
 - запись журнала контроля (QAUDJRN) 302
 - превышено ограничение для учетной записи (VL), формат файла 721
 - предоставить дескриптор (GS), формат файла 644
 - Предоставить пользователю права доступа (GRTUSRAUT), команда
 - копирование прав доступа 127
 - описание 330
 - переименование профайла 132
 - рекомендации 173
 - Предоставить права доступа к объекту (GRTOBJAUT), команда 167, 328
 - влияние на существующие права доступа 170
 - несколько объектов 169
 - Предоставить права доступа пользователю (GRTUSRPMN), команда 332
 - предоставление
 - пользователь, права доступа 332
 - права доступа к объектам 328
 - влияние на существующие права доступа 170
 - несколько объектов 169
 - права доступа на основе модельного объекта 173
 - права доступа пользователя
 - описание команды 330
 - предотвращение появления профайлов больших размеров
 - планирование приложений 237
 - предупреждение
 - права доступа к объектам, необходимые для применения команд 373
 - предупреждение, описание
 - права доступа к объектам, необходимые для применения команд 373
 - преобразование при восстановлении (QFRCCVNRST)
 - системное значение 47
 - прерывать (*BREAK), режим доставки пользовательский профайл 107
 - прерывающее сообщение, программа обработки
 - принятые права доступа 158
 - прикладной программный интерфейс (API)
 - уровень защиты 40 16
 - приложение, разработка
 - библиотеки 236
 - игнорирование принятых прав доступа 245
 - меню 240
 - общие рекомендации по защите 232
 - принятые права доступа 242, 246
 - профайлы 237
 - списки библиотек 238
 - Применять принятые права доступа (QUSEADPAUT), системное значение
 - описание 38
 - риск изменения 39

Применять принятые права доступа (USEADPAUT), параметр 160
 пример
 JKL Toys, приложения 231
 RSTLICPGM (Восстановить лицензионную программу), команда 267
 включение пользовательского профайла 130
 защита библиотек
 описание 240
 планирование 237
 защита меню
 описание 241, 242
 защита очередей вывода 224
 игнорирование принятых прав доступа 245
 изменение
 системная часть списка библиотек 239
 уровни поддержки 85
 общие права доступа
 создание объектов 146
 ограничение доступа к командам сохранения и восстановления 228
 описание
 защита библиотек 240
 защита меню 241, 242
 права доступа, проверка
 группа, права доступа 196
 игнорирование прав доступа группы 200
 общие права доступа 198, 201
 основная группа 196
 принятые права доступа 199, 201
 список прав доступа 202
 принятые права доступа
 права доступа, процесс проверки 199, 201
 приложение, разработка 242, 246
 программа выхода проверки паролей 65
 программа проверки пароля 65
 список библиотек
 защита, риск 218
 изменение системной части 239
 программа 238
 управление пользовательской частью 238
 управление
 пользовательский список библиотек 238
 уровень поддержки
 изменение 85
 принадлежность
 ALWOBJDIF (Разрешить различия в объектах), параметр 264
 OWNER, параметр пользовательского профайла
 описание 103
 блок-схема 184
 буферный файл 222
 введение 5
 восстановление 259, 263
 группа, профайл 150
 принадлежность (*продолжение*)
 изменение
 запись журнала контроля (QAUDJRN) 298
 необходимые права доступа 150
 способы 171
 изменение при восстановлении 263
 запись журнала контроля (QAUDJRN) 293
 новый объект 152
 объекта
 управление 255
 частные права доступа 137
 описание 149
 описание устройства 213
 по умолчанию (QDFTOWN), пользовательский профайл 152
 принтер, вывод 222
 принятые права доступа 158
 присвоение новым объектам 152
 работа с 171
 рабочая станция 213
 сохранение 259
 удаление
 владелец, профайл 127, 150
 управление
 владелец, размер профайла 150
 принадлежность объекта
 ALWOBJDIF (Разрешить различия в объектах), параметр 264
 блок-схема 184
 восстановление 259, 263
 группа, профайл 150
 изменение
 запись журнала контроля (QAUDJRN) 298
 необходимые права доступа 150
 описание команды 328
 перенос приложений в рабочую среду 255
 способы 171
 изменение при восстановлении 263
 обязанности 275
 описание 149
 принятые права доступа 158
 работа с 171, 328
 сохранение 259
 удаление
 владелец, профайл 127, 150
 управление
 владелец, размер профайла 150
 частные права доступа 137
 принимающие программы
 просмотр 322
 принтер (DEV), параметр
 пользовательский профайл 108
 принтер, вывод
 *JOBCTL (управление заданиями), специальные права доступа 91
 *SPLCTL (управление буфером), специальные права доступа 91
 владелец 222
 защита 221, 222
 права доступа к объектам, необходимые для применения команд 508
 принятие прав доступа владельца 276
 принятие прав доступа программой (PA), тип записи журнала 298
 принятие прав доступа программой (PA), формат файла 680
 принятые
 права доступа
 просмотр 163
 принятые права доступа
 *PGMADP (принятие программой прав доступа), уровень контроля 292
 AP (принятые права доступа), тип записи журнала 292
 AP (принятые права доступа), формат файла 611
 Attention (ATTN), клавиша 158
 блок-схема 191
 восстановление программ
 изменения принадлежности и прав доступа 267
 группа, права доступа 157
 задание, инициализация 211
 запись журнала контроля (QAUDJRN) 292, 611
 защита библиотек 142
 игнорирование 160, 245
 изменение
 job 158
 запись журнала контроля (QAUDJRN) 298
 необходимые права доступа 158
 определение 156
 отладка, функции 158
 параметров контроля 276
 переход к групповому заданию 158
 печать списка объектов 754
 права доступа, пример проверки 199, 201
 прерывающее сообщение, программа обработки 158
 приложение, разработка 242, 245, 246
 пример 242, 245, 246
 принадлежность объекта 158
 просмотр
 USRPRF, параметр 159
 важные файлы 248
 описание команды 331
 программы, принимающие профайл 159
 рекомендации 159
 риски 159
 связанные программы 159
 системный запрос, функция 158
 служебные программы 159
 создание программы 158
 специальные права доступа 157
 цель 156
 принятые права доступа (*ADOPTED) 163
 приоритет 229
 приоритет планирования
 ограничение 100
 присвоение имени
 группа, профайл 79, 80
 получатель журнала контроля 309
 пользовательский профайл 79, 80
 Проверить пароль (CHKPWD), команда 133, 329

Проверить целостность объекта (CHKOBJTG), команда контроль использования 277
 описание 322, 330, 754
 проверка
 восстановленные программы 18
 проверка параметров 18
 проверка программы
 определение 18
 проверка совпадения паролей (QPWDRQDDIF), системное значение значение, устанавливаемое командой CFGSYSSEC 759
 проверка соединения (CV), формат файла 624
 программа
 восстановление
 контрольное значение 18
 принятые права доступа 267
 риски 266
 запрет
 несанкционированный 277
 игнорирование
 принятые права доступа 160
 изменение
 настройка параметра USEADPAUT 160
 несанкционированный 277
 перемещение
 принятые права доступа 157
 права доступа к объектам, необходимые для применения команд 490
 принятые права доступа
 восстановление 267
 запись журнала контроля (QAUDJRN) 298
 игнорирование 160
 параметров контроля 276
 перемещение 157
 просмотр 159
 создание 158
 цель 156
 проверка паролей
 QPWDVLDPGM, системное значение 63
 пример 65
 требования 64
 программа выхода проверки паролей
 пример 65
 программный сбой
 запись журнала контроля (QAUDJRN) 298
 просмотр
 принятые права доступа 159
 работа с пользовательскими профайлами 133
 связанная
 принятые права доступа 159
 служебная
 принятые права доступа 159
 создание
 принятые права доступа 158
 трансляция 18
 триггер
 полный список 334
 программа (продолжение)
 функция принятия прав доступа параметров контроля 322
 программа (*PGM), контроль 571
 программа Attention операционной поддержки
 программа обработки клавиши Attention 110
 программа выхода 65
 программа обработки клавиши Attention *ASSIST 110
 QATNPGM, системное значение 110
 QEZMAIN, программа 110
 задание 109
 задание, инициализация 210
 изменение 110
 командный процессор QCMD 109
 начальная программа 109
 пользовательский профайл 109
 программа подтверждения паролей (QPWDVLDPGM), системное значение 63
 программа подтверждения, пароль 64, 65
 программа проверки, пароль 64, 65
 программа системы
 прямой вызов 16
 программа триггера
 полный список 334, 754
 программа чтения
 права доступа к объектам, необходимые для применения команд 496
 программирование, язык
 права доступа к объектам, необходимые для применения команд 450
 программист
 контроль доступа к рабочим библиотекам 274
 приложение
 планирование защиты 254
 системный
 планирование защиты 256
 программист, пользовательский профайл (QPGMR)
 значения по умолчанию 339
 описание устройства, владелец 213
 программный сбой
 восстановление программ
 запись журнала контроля (QAUDJRN) 293
 параметров контроля 322
 производительность
 вывод, приоритет 229
 выполнение заданий только в пакетном режиме 229
 задание, описание 229
 задание, планирование 229
 запись маршрутизации 229
 запуск, приоритет 229
 квант времени 229
 класс 229
 описание подсистемы 229
 память
 пул 229
 производительность (продолжение)
 права доступа к объектам, необходимые для применения команд 482
 приоритет, ограничение 229
 пул 229
 производительность, настройка
 защита 229
 прокрутка
 инверсия (*ROLLKEY, опция пользователя) 114
 промежуточный уровень поддержки 78, 85
 просмотр
 CRTAUT (права при создании), параметр 165
 QAUDCTL (управление контролем), системное значение 334, 751
 QAUDLVL (уровень контроля), системное значение 334, 751
 буферный файл 222
 владельцев прав доступа 160
 описание команды 327
 все пользовательские профайлы 130
 журнал
 контроль операций с файлами 248, 319
 задание, описание 276
 записи журнала контроля 313, 334
 записи журнала контроля (QAUDJRN) 278, 313
 информация о входе в систему
 DSPSGNINF пользовательский профайл, параметр 96
 QDSPSGNINF, системное значение 29
 рекомендации 96
 контроль действий 334, 751
 контроля объекта 306
 объект домена 16
 объекта
 инициатор 151
 описание объекта 328
 полное имя 172
 пользователи с правами доступа 320, 330
 пользовательский профайл
 описание команды 330
 отдельный 130
 расписание активации 749
 расписание истечения срока 749
 список активных профайлов 749
 список сводной информации 130
 права доступа 162, 328
 права доступа к объектам 321, 328
 права доступа к объекту библиотеки документов 332
 принимающие программы 159, 322
 принятие прав доступа программой 159
 принятые права доступа
 USRPRF, параметр 159
 важные файлы 248
 описание команды 331
 программы, принимающие профайл 159
 режим программы 16

- просмотр (*продолжение*)
- Показать программу (DSPPGM), команда 16
 - список прав доступа
 - объекты библиотеки документов (DLO) 332
 - пользователи 327
 - список прав доступа, объекты 176, 327
- протоколы Secure Sockets Layer (SSL) (QSSLPCL), системное значение 44
- профайл
- AUDLVL (контроль действий) 118
 - OBJAUD (контроль за объектом) 117
 - QDFTOWN (владелец по умолчанию)
 - восстановление программ 267
 - анализ с помощью запроса 320
 - группа 274
 - введение 5, 78
 - защита ресурсов 5
 - параметров контроля 274
 - пароль 80
 - планирование 251
 - принадлежность объекта 150
 - присвоение имени 80
 - изменение 330
 - контроль действий (AUDLVL) 118
 - контроль за объектом (OBJAUD) 117
 - контроль пароля 274
 - контроль членства 274
 - обработка
 - запись журнала контроля (QAUDJRN) 299
 - параметров контроля
 - *ALLOBJ, специальные права доступа 274
 - права на использование 275
 - пользователь 117, 118, 320
 - ACGCDE (код учета ресурсов) 105
 - ASTLVL (уровень поддержки) 84
 - ATNPGM (программа обработки клавиши Attention) 109
 - CCSID (идентификатор набора символов) 111
 - CHRIDCTL (опции пользователя) 112
 - CNTRYID (идентификатор страны или региона) 111
 - CURLIB (текущая библиотека) 85
 - DEV (принтер) 108
 - DLVRY (доставка в очередь сообщений) 107
 - DOCPWD (пароль документа) 106
 - DSPSGNINF (информация о входе в систему) 96
 - GRPAUT (права доступа группы) 103, 150
 - GRPAUTTYPR (тип прав доступа группы) 104
 - GRPPRF (группа) 102
 - INLMNU (начальное меню) 87
 - INLPGM (начальная программа) 86
 - JOB (описание задания) 101
 - KBDBUF (буферизация клавиатуры) 98
- профайл (*продолжение*)
- пользователь (*продолжение*)
 - LANGID (идентификатор языка) 111
 - LCLPDMGMT (локальное управление паролем) 97
 - LMTCPB (ограничить возможности) 88
 - LMTDEVSSN (ограничить сеансы одним устройством) 98
 - LOCALE (опции пользователя) 113
 - MAXSTG (максимальный объем памяти) 99
 - MSGQ (очередь сообщений) 106
 - OUTQ (очередь вывода) 108
 - PTYLMT (ограничение приоритета) 100
 - PWDEXP (ограничить срок действия пароля) 82
 - PWDEXPITV (срок действия пароля) 96
 - SETJOBATR (опции пользователя) 112
 - SEV (серьезность очереди сообщений) 108
 - SPCAUT (специальные права доступа) 89
 - SPCENV (специальная среда) 94
 - SRTSEQ (последовательность сортировки) 110
 - SUPGRPPRF (дополнительные группы) 105
 - user identification number 114
 - USRCLS (класс пользователя) 83
 - USROPT (опции пользователя) 112, 113
 - USRPRF (имя) 79
 - автоматическое создание 77
 - большой, проверка 321
 - буферизация клавиатуры (KBDBUF) 98
 - введение 4
 - владелец создаваемых объектов (OWNER) 103, 150
 - группа (GRPPRF) 102
 - домашний каталог (HOMEDIR) 115
 - дополнительные группы (SUPGRPPRF) 105
 - доставка (DLVRY) 107
 - доставка в очередь сообщений (DLVRY) 107
 - загрузка 133
 - идентификатор набора символов (CCSID) 111
 - идентификатор страны или региона (CNTRYID) 111
 - идентификатор языка (LANGID) 111
 - изменение 127
 - имя (USRPRF) 79
 - класс пользователя (USRCLS) 83
 - код учета ресурсов (ACGCDE) 105
 - локальное управление паролем (LCLPDMGMT) 97
- профайл (*продолжение*)
- пользователь (*продолжение*)
 - максимальный объем памяти (MAXSTG) 99
 - начальная программа (INLPGM) 86
 - начальное меню (INLMNU) 87
 - номер ИД группы, (GID) 114
 - общие права доступа (AUT) 117
 - ограничение возможностей 88, 274
 - ограничение приоритета (PTYLMT) 100
 - ограничить сеансы одним устройством (LMTDEVSSN) 98
 - ограничить срок действия пароля (PWDEXP) 82
 - описание (TEXT) 89
 - описание задания (JOB) 101
 - опции пользователя (CHRIDCTL) 112
 - опции пользователя (LOCALE) 113
 - опции пользователя (SETJOBATR) 112
 - опции пользователя (USROPT) 112, 113
 - очередь вывода (OUTQ) 108
 - очередь сообщений (MSGQ) 106
 - параметров контроля 274
 - пароль 80
 - пароль документа (DOCPWD) 106
 - переименование 131
 - показать информацию о входе в систему (DPSGNINF) 96
 - последовательность сортировки (SRTSEQ) 110
 - поставляемый IBM 134
 - права доступа (AUT) 117
 - права доступа группы (GRPAUT) 103, 150
 - принтер (DEV) 108
 - присвоение имени 80
 - программа обработки клавиши Attention (ATNPGM) 109
 - роли 77
 - связь eim (EIMASSOC) 115
 - серьезность (SEV) 108
 - серьезность очереди сообщений (SEV) 108
 - состояние (STATUS) 83
 - специальная среда (SPCENV) 94
 - специальные права доступа (SPCAUT) 89
 - список выбранных 320
 - список неактивных 320
 - список пользователей с правами на выполнение команд 320
 - список пользователей со специальными правами доступа 320
 - среда System/36 94
 - срок действия пароля (PWDEXPITV) 96
 - текст (TEXT) 89
 - текущая библиотека (CURLIB) 85
 - тип прав доступа группы (GRPAUTTYPR) 104

профайл (*продолжение*)
 пользователь (*продолжение*)
 уровень поддержки (ASTLVL) 84
 поставляемый IBM
 BRM, пользовательский профайл
 QBRMS 339
 IBM, профайл прав доступа
 QAUTPROF 339
 QAUTPROF (профайл прав доступа IBM) 339
 QBRMS (пользовательский профайл BRM) 339
 QDBSHR (общая база данных) 339
 QDFTOWN (владелец по умолчанию) 339
 QDOC (документ) 339
 QDSNX (узловой исполнитель в распределенных системах) 339
 QFNC (финансы) 339
 QGATE (мост VM/MVS) 339
 QLPAUTO (автоматическая установка лицензионной программы) 339
 QLPINSTALL (установка лицензионных программ) 339
 QMSF (среда почтового сервера) 339
 QNFANON (сетевая файловая система) 339
 QPGMR (программист) 339
 QRJE (запись удаленного задания) 339
 QSECOFR (системный администратор) 339
 QSNADS (службы рассылки системной сетевой архитектуры) 339
 QSPL (буфер) 339
 QSPLJOB (буферное задание) 339
 QSRV (служба) 339
 QSRVBAS (базовый профайл обслуживания) 339
 QSYS (система) 339
 QSYSOPR (системный оператор) 339
 QTCP (TCP/IP) 339
 QTMPLPD (поддержка печати по TCP/IP) 339
 QTSTRQS (тестовый запрос) 339
 QUSER (пользователь рабочей станции) 339
 TCP/IP (QTCP) 339
 автоматическая установка (QLPAUTO) 339
 базовый профайл обслуживания (QSRVBAS) 339
 буфер (QSPL) 339
 буферное задание (QSPLJOB) 339
 владелец по умолчанию (QDFTOWN) 339
 документ (QDOC) 339
 запись удаленного задания (QRJE) 339
 команды с ограниченным доступом 347
 мост VM/MVS (QGATE) 339
 общая база данных (QDBSHR) 339

профайл (*продолжение*)
 поставляемый IBM (*продолжение*)
 параметров контроля 272
 поддержка печати по TCP/IP (QTMPLPD) 339
 пользователь рабочей станции (QUSER) 339
 права доступа, профайл QAUTPROF 339
 программист (QPGMR) 339
 сетевая файловая система (QNFS) 339
 система (QSYS) 339
 системный администратор (QSECOFR) 339
 системный оператор (QSYSOPR) 339
 служба (QSRV) 339
 службы рассылки SNA (QSNADS) 339
 среда почтового сервера (QMSF) 339
 тестовый запрос (QTSTRQS) 339
 узловой исполнитель в распределенных системах (QDSNX) 339
 установка лицензионных программ (QLPINSTALL) 339
 финансы (QFNC) 339
 смена
 запись журнала контроля (QAUDJRN) 299
 таблица значений по умолчанию 337
 пул 229

Р

работа от имени
 параметров контроля 562
 работа с
 атрибуты журнала 312, 319
 буферные файлы 222
 владельцы прав доступа 327, 332
 журнал 319
 каталог 333
 объекты 328
 объекты библиотеки документов (DLO) 332
 объекты по владельцу 328
 объекты по основной группе 152, 328
 основная группа 172
 очередь вывода, описание 222
 пароль 329
 пользовательских профайлов 122, 330, 331
 права доступа 328
 права доступа к объектам 328
 принадлежность объекта 171
 система, состояние 229
 системный каталог 333
 списков прав доступа 327
 средства контроля пользователей 132
 Работа с атрибутами журнала (WRKJRNA), команда 312, 319
 Работа с буферными файлами (WRKSPLF), команда 222
 Работа с журналом (WRKJRN), команда 312, 319
 Работа с каталогом (WRKDIRE), команда 333
 Работа с объектами (WRKOBJ), команда 328
 Работа с объектами по владельцу (WRKOBJOWN), команда
 использование 171
 описание 328
 параметров контроля 275
 Работа с объектами по владельцу, меню 128, 171
 Работа с объектами по основной группе (WRKOBJPGP), команда 152, 172
 описание 328
 Работа с описанием очереди вывода (WRKOUTQD), команда 222
 Работа с правами доступа (WRKAUT), команда 167, 328
 Работа с регистрацией пользователей, меню 123
 Работа с системными значениями (WRKSYSVAL), команда 272
 Работа с состоянием системы (WRKSYSSTS), команда 229
 Работа с файлами базы данных с помощью IDDU (WRKDBFIDD), команда
 необходимые права доступа к объектам 435
 Работа со списками прав доступа (WRKAUTL), команда 327
 рабочая библиотека
 рекомендации 220
 список библиотек 220
 описание 218
 рабочая станция
 защита 211
 ограничение доступа 272
 ограничения на одно устройство 31
 права доступа системного администратора 32
 права на вход в систему 211
 рабочая станция, запись
 вход в систему без ИД пользователя и пароля 17
 задание, описание 216
 разработка
 библиотеки 236
 защита 231
 разрешение
 на изменение паролей пользователями 273
 разрешение применения QSECOFR (пользовательский профайл системного администратора) 83
 пользовательский профайл автоматически 749
 пример программы 130
 разрешения
 определение 140
 разрешенная функция
 ограничить возможности (LMTCPB) 88
 разрешить восстановление объектов (QALWOBJRST), системное значение 48

разрешить восстановление объектов (QALWBJRST), системное значение *(продолжение)*
 значение, устанавливаемое командой CFGSYSSEC 759

разрешить для пользователя с ограниченными возможностями (ALWLMTUSR), параметр
 Изменить команду (CHGCMD), команда 88
 ограничение возможностей 88
 Создать команду (CRTCMD), команда 88

разрешить пользовательские объекты (QALWUSRDMN), системное значение 21, 27

разрешить различия в объектах (ALWBJDIF), параметр 264

разрешить удаленный вход в систему (QRMTSIGN), системное значение
 значение, устанавливаемое командой CFGSYSSEC 759

расписание заданий
 права доступа к объектам, необходимые для применения команд 443

рассылка
 права доступа к объектам, необходимые для применения команд 395

рассылка, системный каталог команды 333

расширение уровня контроля (QAUDLVL2), системное значение 72

расширенная аппаратная защита памяти
 запись журнала контроля (QAUDJRN) 292
 уровень защиты 40 18

расширенная беспроводная локальная сеть, настройка
 права доступа к объектам, необходимые для применения команд 403

расширенный (*ADVANCED) уровень поддержки 78, 85

регистрация
 пользователи 123

редактирование
 объект библиотеки документов (DLO)
 права доступа 332
 права доступа к объектам 167, 328
 список библиотек 218
 список прав доступа 175, 327

Редактировать права доступа к объекту
 отображение сведений (*EXPERT, опция пользователя) 112, 113, 114

Редактировать права доступа к объекту (EDTOBJAUT), команда 167, 328

Редактировать права доступа к объекту библиотеки документов (EDTDLOAUT), команда 332

Редактировать список прав доступа (EDTAUTL), команда 175, 327

режим
 программа 16

режим доступа
 определение 138

режим программы
 определение 16
 просмотр 16

резервное копирование
 информации о защите 259
 права доступа к объектам, необходимые для применения команд 477

рекомендация
 QUSRLIBL, системное значение 102
 RSTLICPGM (Восстановить лицензионную программу), команда 267
 библиотека, разработка 236
 класс пользователя (USRCLS) 84
 начальная программа (INLPGM) 88
 начальное меню (INLMNU) 88
 начальный список библиотек 102
 обзор 232
 общие права доступа
 пользовательских профайлов 117
 ограничение
 сеансов одним устройством 98
 ограничение приоритета (PTYLMT), параметр 101
 ограничить возможности (LMTCPB) 88
 ограничить срок действия пароля (PWDEXP) 82
 описания заданий 102
 пароли 81
 показать информацию о входе в систему (DSPSGNINF) 96
 приложение, разработка 237
 принятые права доступа 159
 присвоение имени
 группа, профайл 80
 пользовательских профайлов 80
 разработка средств защиты 232
 сообщения, очередь 107
 специальная среда (SPCENV) 94
 специальные права доступа (SPCAUT) 94
 список библиотек
 пользовательская часть 221
 рабочие библиотеки, список 220
 системная часть 220
 текущая библиотека 220
 срок действия пароля (PWDEXPITV) 96
 уровень защиты (QSECURITY), системное значение 11

реляционная база данных, каталог
 права доступа к объектам, необходимые для применения команд 497

ресурс
 права доступа к объектам, необходимые для применения команд 497

ресурс шрифта (*FNTRSC), контроль за объектом 554

риск
 *ALLOBJ (ко всем объектам), специальные права доступа 90
 *AUDIT (контроль), специальные права доступа 93

риск *(продолжение)*
 *IOSYSCFG (конфигурация системы), специальные права доступа 94
 *JOBCTL (управление заданиями), специальные права доступа 91
 *SAVSYS (специальные права на сохранение системы) 92
 *SERVICE, специальные служебные права доступа 92
 *SPLCTL (управление буфером), специальные права доступа 91
 RSTLICPGM (Восстановить лицензионную программу), команда 267
 владелец прав доступа 162
 восстановление программ 267
 восстановление программ, принимающих права доступа 267
 восстановление, команды 227
 права при создании (CRTAUT), параметр 146
 принятые права доступа 159
 программа проверки пароля 64
 сохранение, команды 227
 специальные права доступа 90
 список библиотек 218

С

сбой
 вход в систему
 *ALLOBJ (ко всем объектам), специальные права доступа 211
 *SERVICE, специальные служебные права доступа 211
 QSECOFR (пользовательский профайл системного администратора) 211

сброс пароля DST (DS), тип записи журнала 294

сброс поставляемого IBM ИД пользователя сервисных средств (DS), формат файла 637

связанная программа
 определение 159
 принятые права доступа 159

связь eim (EIMASSOC), параметр
 пользовательский профайл 115

сеанс
 права доступа к объектам, необходимые для применения команд 498

сеанс сервера
 запись журнала контроля (QAUDJRN) 289

сеанс сервера (VS), тип записи журнала 289

сеанс сервера (VS), формат файла 727

сеанс устройства
 ограничение
 LMTDEVSSN пользовательский профайл, параметр 98
 QLMTDEVSSN, системное значение 31

сегмент страницы (*PAGSEG), контроль 570

- сервер каталогов
 - параметров контроля 542
 - права доступа к объектам, необходимые для применения команд 394
- Сервер каталогов (DI), формат файла 629
- сервер хоста
 - права доступа к объектам, необходимые для применения команд 413
- сервер, идентификация
 - права доступа к объектам, необходимые для применения команд 502
- сервисные средства (*SERVICE), уровень контроля 301
- серьезность (SEV), параметр пользовательский профайл 108
- сетевой атрибут
 - *SECADM (администратор защиты), специальные права доступа 90
 - DDMACC (доступ к DDM) 277
 - DDMACC (обработка запросов DDM) 227
 - JOBACN (действие над заданием) 225, 277
 - PC Support (PCSACC) 277
 - PCSACC (доступ к PC Support) 277
 - PCSACC (обработка запросов клиентов) 226
 - действие над заданием (JOBACN) 225, 277
 - доступ к DDM (DDMACC) 277
 - изменение
 - запись журнала контроля (QAUDJRN) 298
 - команда 225
 - клиент, обработка запросов (PCSACC) 226
 - команда настройки 335, 759
 - Обработка запросов DDM (DDMACC) 227
 - печать влияющих на защиту 754
 - права доступа к объектам, необходимые для применения команд 471
- сетевой интерфейс (*NWID), контроль 567
- сетевой интерфейс, описание
 - права доступа к объектам, необходимые для применения команд 473
- сетевой профайл
 - изменение
 - запись журнала контроля (QAUDJRN) 299
- сетевой сервер
 - права доступа к объектам, необходимые для применения команд 473
- сетевые атрибуты
 - печать влияющих на защиту 335
 - печать параметров защиты средств связи 335
- сеть
 - вход
 - запись журнала контроля (QAUDJRN) 289
 - выход
 - запись журнала контроля (QAUDJRN) 289
 - пароль
 - запись журнала контроля (QAUDJRN) 288
- сеть, буферный файл
 - отправка 222
- символы
 - пароль 52
- символы в одинаковых позициях (QPWDPOSDIF), системное значение 57
- символы пароля 52
- символьная ссылка (*SYMLNK), контроль 586
- система (*SYSTEM), домен 16
- система (*SYSTEM), режим 16
- система (QSYS), пользовательский профайл
 - восстановление 263
 - значения по умолчанию 339
- система, консоль 213
 - QCONSOLE, системное значение 213
- система, состояние
 - работа с 229
- системная библиотека QSYS
 - списков прав доступа 145
- системная библиотека, список
 - QSYSLIBL, системное значение 218
 - изменение 218, 239
- Системная сетевая архитектура (SNA)
 - службы рассылки (QSNADS), пользовательский профайл 339
- системная часть
 - список библиотек
 - изменение 239
 - описание 218
 - рекомендации 220
- системное значение
 - QALWBJRST (разрешить восстановление объектов) 48
 - значение, устанавливаемое командой CFGSYSSEC 759
 - QALWUSRDMN (разрешить пользовательские объекты) 21, 27
 - QATNPGM (программа обработки клавиши Attention) 110
 - QAUDCTL (управление контролем)
 - изменение 334, 751
 - обзор 69
 - просмотр 334, 751
 - QAUDENDACN (действие при сбое контроля) 69, 307
 - QAUDFRCLVL (уровень выгрузки записей контроля) 70, 306
 - QAUDLVL (уровень контроля)
 - *AUTFAIL (ошибка прав доступа), описание 286
 - *CREATE (создание), значение 288
 - *DELETE (удаление), значение 288
 - *JOBDDTA (изменение задания), значение 289
- системное значение (продолжение)
 - QAUDLVL (уровень контроля) (продолжение)
 - *OBJMGT (управление объектом), значение 291
 - *OFCSRV (функции Office), значение 291
 - *PGMADP (принятые права доступа), значение 292
 - *PGMFAIL (сбой программы), значение 292
 - *PRTDDTA (печатаемый вывод), значение 293
 - *SAVRST (сохранение/восстановление), значение 293
 - *SECURITY (защита), значение 297
 - *SERVICE (сервисные средства), значение 301
 - *SPLFDDTA (изменения буферного файла), значение 301
 - *SYSMGT (управление системами), значение 301
 - изменение 309, 334, 751
 - обзор 71
 - пользовательский профайл 118
 - просмотр 334, 751
 - цель 278
 - QAUDLVL2 (расширение уровня контроля)
 - обзор 72
 - QAUTOCFG (автоматическая настройка устройств) 40
 - QAUTOCFG (автоматическая настройка)
 - значение, устанавливаемое командой CFGSYSSEC 759
 - QAUTOVRT (автоматическая настройка виртуальных устройств) 41
 - значение, устанавливаемое командой CFGSYSSEC 759
 - QCCSID (идентификатор набора символов) 112
 - QCNTYID (идентификатор страны или региона) 111
 - QCONSOLE (консоль) 213
 - QCRTAUT (права при создании)
 - использование 146
 - описание 28
 - риск изменения 28
 - QCRTOBJAUD (создать контроль за объектом) 74
 - QDEVRCYACN (действие для восстановления устройства)
 - значение, устанавливаемое командой CFGSYSSEC 759
 - QDSCJOBITV (тайм-аут отключенного задания) 42
 - значение, устанавливаемое командой CFGSYSSEC 759
 - QDSPSGNINF (показать информацию о входе в систему) 29, 96
 - значение, устанавливаемое командой CFGSYSSEC 759
 - QFRCCVNRST (преобразование при восстановлении) 47

системное значение (*продолжение*)

QINACTITV (тайм-аут неактивного задания) 29
 значение, устанавливаемое командой CFGSYSSEC 759

QINACTMSGQ (очередь сообщений неактивного задания) 30
 значение, устанавливаемое командой CFGSYSSEC 759

QKBDBUF (буферизация клавиатуры) 99

QLANGID (идентификатор языка) 111

QLMTDEVSSN (ограничить сеансы одним устройством)
 LMTDEVSSN пользовательский профайл, параметр 98
 параметров контроля 274

QLMTSECOFR (ограничить права системного администратора)
 вход в систему 213
 значение, устанавливаемое командой CFGSYSSEC 759
 изменение уровня защиты 14
 описание 32
 параметров контроля 272
 права доступа к описаниям устройств 211

QMAXSGNACN (действие при достижении максимального числа попыток входа в систему)
 значение, устанавливаемое командой CFGSYSSEC 759
 описание 33
 состояние пользовательского профайла 83

QMAXSIGN (максимальное число попыток входа в систему)
 значение, устанавливаемое командой CFGSYSSEC 759
 описание 32
 параметров контроля 272, 276
 состояние пользовательского профайла 83

QPRTEDEV (принтер) 108

QPWDCHGBLK (блокировка изменения пароля)
 описание 51

QPWDEXPITV (срок действия пароля)
 PWDEXPITV пользовательский профайл, параметр 96
 значение, устанавливаемое командой CFGSYSSEC 759
 описание 51
 параметров контроля 273

QPWDEXPWRN (предупреждение об истечении срока действия пароля)
 описание 52

QPWDLMTAJC (запрет цифр в соседних позициях в пароле)
 значение, устанавливаемое командой CFGSYSSEC 759

QPWDLMTAJC (запретить применение последовательности цифр) 55

QPWDLMTCHR (запретить некоторые символы) 55

системное значение (*продолжение*)

QPWDLMTCHR (недопустимые для пароля символы)
 значение, устанавливаемое командой CFGSYSSEC 759

QPWDLMTREP (запрет повторяющихся символов в пароле)
 значение, устанавливаемое командой CFGSYSSEC 759

QPWDLMTREP (запретить повторяющиеся символы) 56

QPWDMAXLEN (максимальная длина пароля) 54
 значение, устанавливаемое командой CFGSYSSEC 759

QPWDMINLEN (минимальная длина пароля) 53
 значение, устанавливаемое командой CFGSYSSEC 759

QPWDRQDDIF (символы в одинаковых позициях) 57

QPWDRQDDGT (обязательное вхождение в пароль цифр) 57

QPWDRQDDGT (требовать наличия цифр в пароле)
 значение, устанавливаемое командой CFGSYSSEC 759

QPWDRQDDIF (обязательное изменение пароля) 54

QPWDRQDDIF (проверка совпадения паролей)
 значение, устанавливаемое командой CFGSYSSEC 759

QPWDLVDPGM (программа проверки пароля) 63
 значение, устанавливаемое командой CFGSYSSEC 759

QRETSVRSEC (сохранить идентификационные данные на сервере) 34

QRMTSIGN (разрешить удаленный вход в систему)
 значение, устанавливаемое командой CFGSYSSEC 759

QRMTSIGN (удаленный вход в систему) 35, 277

QRMTSRVATR (атрибут удаленного обслуживания) 42

QSCANFS (сканирование в файловых системах) 36

QSCANFCTL (управление сканированием в файловых системах) 36

QSECURITY (уровень защиты)
 автоматическое создание пользовательских профайлов 77
 введение 2
 внутренние управляющие блоки 22
 значение, устанавливаемое командой CFGSYSSEC 759
 класс пользователя 11
 обзор 9
 обработка сообщений 21
 отключение уровня 40 20
 отключение уровня 50 22
 параметров контроля 272

системное значение (*продолжение*)

QSECURITY (уровень защиты) (*продолжение*)
 переход на уровень 40 19
 переход, на уровень 20 с более высокого 13
 переход, на уровень 50 22
 переход, с уровня 10 на уровень 20 13
 переход, с уровня 20 на уровень 30 13
 применение системного значения QLMTSECOFR 213
 проверка параметров 18
 рекомендации 11
 специальные права доступа 11
 сравнение уровней 9
 уровень 10 12
 уровень 20 12
 уровень 30 13
 уровень 40 14
 уровень 50 20

QSHRMEMCTL (управление общей памятью)
 возможные значения 38
 описание 38

QSPCENV (специальная среда) 94

QSRTSEQ (последовательность сортировки) 110

QSSLCSL (список шифров SSL) 43

QSSLCSLCTL (управление шифрами SSL) 44

QSSLPCL (протоколы SSL) 44

QSYSLIBL (список системных библиотек) 218

QUSEADPAUT (Применять принятые права доступа)
 описание 38
 риск изменения 39

QUSRLIBL (список пользовательских библиотек) 102

QVFYOBJRST (проверять объект при восстановлении) 45
 автоматическая настройка виртуальных устройств (QAUTOVRT) 41
 автоматическая настройка устройств (QAUTOCFG) 40
 атрибут удаленного обслуживания (QRMTSRVATR) 42
 блокировка изменения пароля (QPWDCHGBLK) 51
 буферизация клавиатуры (QKBDBUF) 99
 вход в систему 52
 действие при достижении максимального числа попыток (QMAXSGNACN) 33, 83
 максимальное число попыток (QMAXSIGN) 32, 83, 272, 276
 удаленный (QRMTSIGN) 35, 277
 действие при достижении максимального числа попыток входа в систему (QMAXSGNACN)
 описание 33
 состояние пользовательского профайла 83

системное значение (*продолжение*)
 действие при сбое контроля
 (QAUDENDACN) 69, 307
 защита
 введение 3
 задание 759
 обзор 26
 идентификатор набора символов
 (QCCSID) 112
 идентификатор страны или региона
 (QCNTRYID) 111
 идентификатор языка (QLANGID) 111
 изменение
 *SECADM (администратор
 защиты), специальные права
 доступа 90
 запись журнала контроля
 (QAUDJRN) 299
 интегрированные файловые системы
 сканирование (QSCANFS) 36
 интегрированные файловые системы,
 управление
 сканирование (QSCANFSTL) 36
 команда настройки 335, 759
 консоль (QCONSOLE) 213
 контроль
 планирование 306
 максимальное число попыток входа в
 систему (QMAXSIGN)
 описание 32
 параметров контроля 272, 276
 состояние пользовательского
 профайла 83
 неактивное задание
 очередь сообщений
 (QINACTMSGQ) 30
 тайм-аут (QINACTITV) 29
 ограничить права системного
 администратора (QLMTSECOFR)
 вход в систему 213
 изменение уровня защиты 14
 описание 32
 права доступа к описаниям
 устройств 211
 ограничить сеансы одним устройством
 (QLMTDEVSSN)
 LMTDEVSSN пользовательский
 профайл, параметр 98
 QLMTDEVSSN (ограничить сеансы
 одним устройством) 31
 описание 31
 параметров контроля 274
 параметров контроля 272
 обзор 68
 пароль
 дубликат (QPWDRQDDIF) 54
 запретить некоторые символы
 (QPWDLMTCHR) 55
 запретить повторяющиеся символы
 (QPWDLMTREP) 56
 запретить применение
 последовательности цифр
 (QPWDLMTJCS) 55
 контроль срока действия 273
 максимальная длина
 (QPWDMAXLEN) 54

системное значение (*продолжение*)
 пароль (*продолжение*)
 минимальная длина
 (QPWDMINLEN) 53
 обзор 49
 обязательное вхождение в пароль
 цифр (QPWDRQDDGT) 57
 предупреждение об истечении срока
 действия (QPWDEXPWRN) 52
 программа подтверждения
 (QPWDVLDPGM) 63
 программа проверки
 (QPWDVLDPGM) 63
 символы в одинаковых позициях
 (QPWDPOSDIF) 57
 срок действия (QPWDEXPITV) 51,
 96
 тривиальный, запрет 273
 печать 272
 печать влияющих на защиту 335, 754
 печать параметров защиты средств
 связи 335
 показать информацию о входе в
 систему (QDPSGGINF) 29, 96
 последовательность сортировки
 (QSRTSEQ) 110
 права доступа к объектам,
 необходимые для применения
 команд 513
 права при создании (QCRTAUT)
 использование 146
 описание 28
 риск изменения 28
 применять принятые права доступа
 (QUSEADPAUT)
 описание 38
 риск изменения 39
 принтер (QPRTEDEV) 108
 проверять восстанавливаемые объекты
 (QVFYOBJRST) 45
 программа обработки клавиши
 Attention (QATNPGM) 110
 Протоколы Secure Sockets Layer (SSL)
 (QSSLPLCL) 44
 работа с 272
 разрешить восстановление объектов
 (QALWOBJRST) 48
 разрешить пользовательские объекты
 (QALWUSRDMN) 21, 27
 расширение уровня контроля
 (QAUDLVL2)
 обзор 72
 связанный с защитой
 обзор 39
 Сканирование в файловых системах
 (QSCANFS) 36
 сканирование в файловых системах
 Scan File Systems 36
 создать контроль за объектом
 (QCRTOBJAUD) 74
 сохранить идентификационные данные
 на сервере (QRETSVRSEC) 34
 специальная среда (QSPCENV) 94
 список 272
 список пользовательских библиотек
 (QUSRLIBL) 102

системное значение (*продолжение*)
 список системных библиотек
 (QSYSLIBL) 218
 Список шифров Secure Sockets Layer
 (SSL) (QSSLCSL) 43
 срок действия пароля (QPWDEXPITV)
 PWDEXPITV пользовательский
 профайл, параметр 96
 тайм-аут для отключенного задания
 (QDSCJOBITV) 42
 удаленный вход в систему
 (QRMTSIGN) 35, 277
 управление в файловых системах
 сканирование (QSCANFSTL) 36
 управление контролем (QAUDCTL)
 обзор 69
 Управление контролем (QAUDCTL)
 изменение 334
 просмотр 334
 управление общей памятью
 (QSHRMEMCTL)
 возможные значения 38
 описание 38
 Управление шифрами Secure Sockets
 Layer (SSL) (QSSLCSLCTL) 44
 уровень выгрузки записей контроля
 (QAUDFRCLVL) 70, 306
 уровень защиты (QSECURITY)
 автоматическое создание
 пользовательских профайлов 77
 введение 2
 класс пользователя 11
 обзор 9
 отключение уровня 40 20
 отключение уровня 50 22
 параметров контроля 272
 переход на уровень 40 19
 переход, на уровень 20 с более
 высокого 13
 переход, на уровень 50 22
 переход, с уровня 10 на уровень
 20 13
 переход, с уровня 20 на уровень
 30 13
 применение системного значения
 QLMTSECOFR 213
 рекомендации 11
 специальные права доступа 11
 сравнение уровней 9
 уровень 10 12
 уровень 20 12
 уровень 30 13
 уровень 40 14
 уровень 50 20
 уровень контроля (QAUDLVL)
 *AUTFAIL (ошибка прав доступа),
 описание 286
 *CREATE (создание), значение 288
 *DELETE (удаление), значение 288
 *JOBDA (изменение задания),
 значение 289
 *OBJMGT (управление объектом),
 значение 291
 *OFCSRV (функции Office),
 значение 291
 *PGMADP (принятые права
 доступа), значение 292

системное значение (*продолжение*)
уровень контроля (QAUDLVL)
(*продолжение*)
*PGMFAIL (сбой программы),
значение 292
*PRTDTA (вывод на принтер),
значение 293
*SAVRST (сохранение/
восстановление), значение 293
*SECURITY (защита),
значение 297
*SERVICE (сервисные средства),
значение 301
*SPLFDTA (изменения буферного
файла), значение 301
*SYSMGT (управление системами),
значение 301
изменение 309, 334
обзор 71
пользовательский профайл 118
просмотр 334
цель 278
файловые системы
сканирование (QSCANFS) 36
системное значение QVFYOBJRST
(проверить объект при
восстановлении) 45
системное значение восстановления
связанный с защитой
обзор 44
системное значение Проверять объект при
восстановлении (QVFYOBJRST) 45
системные операции
специальные права доступа (SPCAUT),
параметр 89
системные права доступа 140
системные ресурсы
ограничение использования
ограничение приоритета (PTYLMT),
параметр 100
предотвращение злоупотреблений 229
системный
права доступа к объектам,
необходимые для применения
команд 512
сохранение 259, 331
системный администратор
ограничение доступа к некоторым
рабочим станциям 272
ограничение доступа к рабочим
станциям 32
отслеживание действий 323
Системный запрос, меню
использование 246
опции и команды 246
системный запрос, функция
принятые права доступа 158
системный информационный код (SRC)
B900 3D10 (ошибка контроля) 70
системный каталог
изменение
запись журнала контроля
(QAUDJRN) 291
системный каталог рассылки
*SECADM (администратор защиты),
специальные права доступа 90
команды 333

системный каталог рассылки
(*продолжение*)
удаление пользовательского
профайла 127
системный оператор (QSYSOPR),
пользовательский профайл 339
системный пароль 137
системный список ответов
права доступа к объектам,
необходимые для применения
команд 513
сканирование в файловых системах
(QSCANFS), системное значение 36
Скопировать буферный файл (CPYSPLF),
команда 222
Скопировать пользователя, меню 126
словарь набора двухбайтовых символов
(*IGCDCT), контроль за объектом 556
службы Office
действие, контроль 562
службы рассылки SNA (SNADS)
QSNADS, пользовательский
профайл 339
служебная
права доступа к объектам,
необходимые для применения
команд 502
служебная программа
принятые права доступа 159
служебная программа (*SRVPGM),
контроль 583
служебная функция изменить
*SERVICE, специальные служебные
права доступа 92
служебная функция показать
*SERVICE, специальные служебные
права доступа 92
служебные права доступа (*SERVICE)
неудачный вход в систему 211
разрешенные функции 92
риски 92
служебный пользовательский профайл
(QSRV)
значения по умолчанию 339
права доступа к консоли 213
смена профайла (PS), тип записи
журнала 299
смена профайла (PS), формат файла 687
совпадающие пароли 54
содержимое
инструменты защиты 334, 749
соединение
включение
запись журнала контроля
(QAUDJRN) 289
выключение
запись журнала контроля
(QAUDJRN) 289
создание
библиотека 165
владелец прав доступа 160, 327, 332
журнал контроля 309
команда
ALWLMTUSR (разрешить для
пользователя с ограниченными
возможностями), параметр 88

создание (*продолжение*)
команда (*продолжение*)
PRDLIB (рабочая библиотека),
параметр 220
риск нарушения безопасности 220
меню
PRDLIB (рабочая библиотека),
параметр 220
риск нарушения безопасности 220
объекта
запись журнала контроля
(QAUDJRN) 151, 288
очередь вывода 222, 224
получатель журнала контроля 309
пользовательский профайл
запись журнала контроля
(QAUDJRN) 294
описания команд 329, 330
пример 123
способы 122
программа
принятые права доступа 158
список прав доступа 174, 327
создание (*CREATE), уровень
контроля 288
создание объекта
контроля объекта 528
создание объекта (CO), тип записи
журнала 151, 288
создание объекта (CO), формат
файла 616
Создать библиотеку (CRTLIB),
команда 165
Создать владельца прав доступа
(CRTAUTHLR), команда 160, 327, 332
Создать журнал (CRTJRN), команда 309
Создать команду (CRTCMD), команда
ALWLMTUSR (разрешить для
пользователя с ограниченными
возможностями), параметр 88
PRDLIB (рабочая библиотека),
параметр 220
риск нарушения безопасности 220
создать контроль за объектом
(CRTOBJAUD), значение 74
создать контроль за объектом
(QCRTOBJAUD), системное значение
обзор 74
Создать контрольные списки
(CRTVLDL) 256
Создать меню (CRTMNU), команда
PRDLIB (рабочая библиотека),
параметр 220
риск нарушения безопасности 220
Создать очередь вывода (CRTOUTQ),
команда 222, 224
Создать получатель журнала
(CRTJRNRCV), команда 309
Создать пользовательский профайл 123
Создать пользовательский профайл
(CRTUSRPRF), команда
использование 123
описание 329, 330
Создать список прав доступа (CRTAUTL),
команда 174, 327

- сокет
 - задание
 - запись журнала контроля (QAUDJRN) 298
 - права доступа к объектам, необходимые для применения команд 373
 - сообщение
 - завершение печати (*PRTMSG, опция пользователя) 114
 - защита
 - отслеживание 317
 - ограничение на содержимое 21
 - состояние
 - не отображается (*NOSTSMMSG, опция пользователя) 114
 - отображается (*STSMMSG, опция пользователя) 114
 - таймер простоя (CPI1126) 30
 - уведомление о печати (*PRTMSG, опция пользователя) 114
 - сообщение о состоянии
 - не отображается (*NOSTSMMSG, опция пользователя) 114
 - отображается (*STSMMSG, опция пользователя) 114
 - сообщение, описание
 - права доступа к объектам, необходимые для применения команд 467
 - сообщения, очередь
 - *BREAK (прерывать), режим доставки 107
 - *DFT (по умолчанию), режим доставки 107
 - *HOLD (блокировать), режим доставки 107
 - *NOTIFY (уведомлять), режим доставки 107
 - QSYMSG 317
 - QMAXSGNACN (действие при достижении максимального числа попыток), системное значение 34
 - QMAXSIGN (максимальное число попыток входа в систему), системное значение 33
 - автоматическое создание 106
 - неактивное задание (QINACTMSGQ), системное значение 30
 - ограничение 217
 - ответ по умолчанию 107
 - пользовательский профайл
 - доставка (DLVRY), параметр 107
 - рекомендации 107
 - серьезность (SEV), параметр 108
 - удаление 127
 - права доступа к объектам, необходимые для применения команд 468
 - рекомендация
 - MSGQ пользовательский профайл, параметр 107
 - серьезность (SEV), параметр 108
 - сортировка набора двухбайтовых символов (*IGCSRT), контроль за объектом 556
- составные
 - права доступа
 - пример 204
 - состояние (STATUS), параметр
 - пользовательский профайл 83
 - сохранение
 - библиотека 259
 - владелец прав доступа 259
 - данные защиты 259, 331
 - информации о защите 259
 - общие права доступа 259
 - объект библиотеки документов (DLO) 259
 - объекта 259
 - ограничение 228
 - основная группа 259
 - параметров контроля 270
 - получатель журнала контроля команды 259
 - принадлежность объекта 259
 - риск нарушения безопасности 227
 - системный 259, 331
 - список прав доступа 259
 - частные права доступа 259
 - сохранение системы (*SAVSYS), специальные права доступа
 - *OBJEXIST, права доступа 138, 360
 - описание 270
 - разрешенные функции 92
 - риски 92
 - удаление системой
 - изменение уровня защиты 13
 - сохранение/восстановление (*SAVRST), уровень контроля 293
 - Сохранить данные защиты (SAVSECDA), команда 259, 331
 - сохранить идентификационные данные на сервере (QRETSVRSEC), значение 34
 - сохранить идентификационные данные на сервере (QRETSVRSEC), системное значение
 - обзор 34
 - Сохранить объект (SAVOBJ), команда 259, 312
 - Сохранить объект библиотеки документов (SAVDLO), команда 259
 - Сохранить систему (SAVSYS), команда 259, 331
 - сочетание различных типов прав доступа
 - пример 204
 - специальная среда (QSPCENV), системное значение 94
 - специальная среда (SPCENV), параметр
 - интерактивное задание
 - выполнения 95
 - рекомендации 94
 - специальная среда *S36 (System/36) 94
 - специальные права доступа
 - *ALLOBJ (все объекты)
 - автоматическое удаление 13
 - добавлено автоматически 13
 - неудачный вход в систему 211
 - параметров контроля 274
 - разрешенные функции 90
 - риски 90
- специальные права доступа (продолжение)
 - *AUDIT (контроль)
 - разрешенные функции 93
 - риски 93
 - *IOSYSCFG (конфигурация системы)
 - разрешенные функции 94
 - риски 94
 - *JOBCTL (управление заданиями)
 - ограничение приоритета (PTYLMT), параметр 100
 - очередь вывода, параметры 223
 - разрешенные функции 91
 - риски 91
 - *SAVSYS (права на сохранение системы)
 - *OBJEXIST, права доступа 138, 360
 - автоматическое удаление 13
 - описание 270
 - разрешенные функции 92
 - риски 92
 - *SECADM (администратор защиты)
 - разрешенные функции 90
 - *SERVICE (служебные)
 - неудачный вход в систему 211
 - разрешенные функции 92
 - риски 92
 - *SPLCTL (управление буфером)
 - очередь вывода, параметры 224
 - разрешенные функции 91
 - риски 91
 - анализ назначения 754
 - добавлено системой
 - изменение уровня защиты 13
 - изменение уровня защиты 13
 - определение 89
 - пользовательский профайл 89
 - права доступа, специальные 253
 - принятые права доступа 157
 - рекомендации 94
 - список пользователей 320
 - удаление системой
 - автоматическое удаление 263
 - изменение уровня защиты 13
 - специальные права доступа (SPCAUT), параметр
 - пользовательский профайл 89
 - рекомендации 94
 - специальные права доступа ко всем объектам (*ALLOBJ)
 - добавлено системой
 - изменение уровня защиты 13
 - неудачный вход в систему 211
 - параметров контроля 274
 - разрешенные функции 90
 - риски 90
 - удаление системой
 - восстановление профайла 263
 - изменение уровня защиты 13
 - специальные права доступа, объединение 253
 - специальные сервисные средства (DST)
 - изменение ИД пользователя 135
 - изменение паролей 135
 - контроль паролей 273

- специальные сервисные средства (DST)
 - (*продолжение*)
 - сброс пароля
 - запись журнала контроля (QAUDJRN) 294
 - описание команды 329
- Специальные сервисные средства (DST)
 - пользователи 134
- Списки прав доступа
 - планирование 174
 - преимущества 174
- списки, создание контрольных 256
- списки, удаление контрольных 256
- список
 - владельцев прав доступа 160
 - все библиотеки 321
 - выбранные пользовательские профайлы 320
 - пользовательский профайл
 - отдельный 130
 - список сводной информации 130
 - системных значений 272
 - содержимое библиотеки 321
- список активных профайлов
 - изменение 749
- список библиотек
 - добавление записей 218, 221
 - изменение 218
 - описание задания (JOBID)
 - пользовательский профайл 101
 - определение 218
 - отслеживание 276
 - пользовательская часть
 - описание 218
 - рекомендации 221
 - управление 238
 - принятые права доступа 142
 - рабочая библиотека
 - описание 218
 - рекомендации 220
 - редактирование 218
 - рекомендации 220
 - риск нарушения безопасности 218
 - системная часть
 - изменение 239
 - описание 218
 - рекомендации 220
 - текущая библиотека
 - описание 218
 - пользовательский профайл 85
 - рекомендации 220
 - удаление записей 218
- список конфигурации, контроль за объектом 533
- список конфигураций
 - права доступа к объектам, необходимые для применения команд 385
- список межсистемных продуктов (*CSPMAP), контроль 537
- список ответов
 - действие, контроль 576
 - права доступа к объектам, необходимые для применения команд 513
- список прав доступа
 - QRCLAUTL (восстановление памяти) 269
 - введение 5
 - восстановление
 - обзор команд 259
 - описание процесса 268
 - связь с объектом 264
 - восстановление памяти (QRCLAUTL) 269
 - восстановление поврежденного 268
 - группа, профайл
 - сравнение 253
 - добавление
 - записи 175, 327
 - объекты 176
 - пользователи 175
 - запись
 - добавление 175
 - защита объектов 176
 - защита поставляемых IBM объектов 145
 - изменение
 - запись 327
 - контроля объекта 531
 - настройка 176
 - объект библиотеки документов (DLO)
 - просмотр 332
 - описание 144
 - печать информации о правах доступа 754
 - поврежденный 268
 - получение записей 327
 - пользователь
 - добавление 175
 - права доступа
 - изменение 175
 - хранение 261
 - права доступа к объектам, необходимые для применения команд 375
 - права доступа, проверка
 - пример 202
 - просмотр
 - объекты 176, 327
 - объекты библиотеки документов (DLO) 332
 - пользователи 327
 - работа с 327
 - редактирование 175, 327
 - создание 174, 327
 - сохранение 259
 - сравнение
 - группа, профайл 253
 - удаление 177, 327
 - записи 327
 - объекты 177
 - пользователи 175, 327
 - управление (*AUTLMGT), права доступа 138, 145, 360
 - хранение
 - права доступа 261
- список рассылки
 - права доступа к объектам, необходимые для применения команд 396
- список рассылки (*продолжение*)
 - удаление пользовательского профайла 127
- список соединений
 - права доступа к объектам, необходимые для применения команд 385
- список соединений (*C>NNL), контроль 536
- список узлов
 - права доступа к объектам, необходимые для применения команд 475
- список узлов (*NODL), контроль 566
- список управления доступом
 - изменение
 - запись журнала контроля (QAUDJRN) 299
- Список шифров Secure Sockets Layer (SSL) (QSSLCSL), системное значение 43
- справочная информация
 - полноэкранный режим (*HLPFULL, опция пользователя) 114
- справочная таблица
 - контроль за действиями 272
 - планирование защиты 272
- сравнение
 - профайл группы и список прав доступа 253
- среда System/36
 - пользовательский профайл 94
 - права доступа к объектам, необходимые для применения команд 513
- среда System/38 94
- среда почтового сервера
 - права доступа к объектам, необходимые для применения команд 464
- среда почтового сервера (QMSF), пользовательский профайл 339
- средства контроля пользователей
 - изменение
 - описание команды 331
 - описания команд 330
- средства связи
 - отслеживание 277
- средства связи, запись
 - задание, описание 216
- срок действия пароля (PWDEXPITV)
 - рекомендации 96
- срок действия пароля (QPWDEXPITV), системное значение
 - параметров контроля 273
- ссылка
 - права доступа к объектам, необходимые для применения команд 378, 415
- существование (*OBJEXIST), права доступа 138, 360
- сфера управления
 - права доступа к объектам, необходимые для применения команд 507

Т

таблица
права доступа к объектам,
необходимые для применения
команд 516

таблица (*TBL), контроль 588

таблица информационных кодов (*RCT),
контроль 576

таблица межсистемных продуктов
(*CSPTBL), контроль 538

таблица набора двухбайтовых символов
(*IGCTBL), контроль за объектом 556

таблица прав доступа 262

таблица предупреждений
права доступа к объектам,
необходимые для применения
команд 373

таблица предупреждений (*ALRTBL),
контроль за объектом 531

таблица управления формами
права доступа к объектам,
необходимые для применения
команд 498

тайм-аут
неактивное задание (QINACTITV),
системное значение 29
очередь сообщений (QINACTMSGQ),
системное значение 30

тайм-аут неактивного задания
(QINACTITV), системное значение
значение, устанавливаемое командой
CFGSYSSEC 759

тайм-аут отключенного задания
(QDSCJOBITV), системное значение 42
значение, устанавливаемое командой
CFGSYSSEC 759

текст (TEXT), параметр
пользовательский профайл 89

текст команды (CD), тип записи
журнала 288

текст команды (*CMD), уровень
контроля 288

текстовая поддержка PC (PCTA)
отключение (системное значение
QINACTMSGQ) 30

текстовый индекс
права доступа к объектам,
необходимые для применения
команд 476

текущая библиотека
изменение
ограничение возможностей 86
рекомендации 221
способы 218

ограничение возможностей 86

определение 85

пользовательский профайл 85
рекомендации 220

список библиотек 218, 220

тестовый запрос (QTSTRQS),
пользовательский профайл 339

тип записи журнала Ошибка прав доступа
(AF) 286
описание 292

тип прав доступа группы
GRPAUTTYR, параметр
пользовательского профайла 104

точки выхода
пользовательский профайл 133

трансляция программ 18

тривиальный пароль

запрет 50, 273

У

уведомление, сообщение
DLVRY (доставка в очередь
сообщений), параметр
пользовательский профайл 107

сообщение об отсутствии состояния
(*NOSTSMSG), опция
пользователя 114

уведомлять (*NOTIFY), режим доставки
пользовательский профайл 107

удаление
библиотека, запись списка 218
владелец прав доступа 161, 327
запись идентификации сервера 332
запись каталога 333
объект, профайл владельца 150
объекта
запись журнала контроля
(QAUDJRN) 288

получатель журнала контроля 312

пользователь, права доступа 169

пользовательский профайл
автоматически 749
буферные файлы 129
запись каталога 127
описание команды 330
основная группа 127
собственные объекты 127
сообщения, очередь 127
списки рассылки 127

права доступа к объекту библиотеки
документов 332

права доступа пользователя 169
объекта 169
список прав доступа 175

сотрудники, которым больше не нужен
доступ 275

список прав доступа 177, 327
объекта 177
права доступа пользователя 175,
327
уровень защиты 40 20
уровень защиты 50 22

удаление (*DELETE), уровень
контроля 288

удаление (*DLT), права доступа 138, 360

удаление объекта
контроля объекта 528

удаленное задание, запуск
защита 225

удаленное подключение
изменение целевого профайла
запись журнала контроля
(QAUDJRN) 299

управление входом в систему 35

удаленный вход в систему
QRMTSIGN, системное значение 35

удаленный вход в систему (QRMTSIGN),
системное значение 35, 277

удаленный вход в систему дисплейной
станции
изменение целевого профайла
запись журнала контроля
(QAUDJRN) 299
права доступа к объектам,
необходимые для применения
команд 394

Удалить владельца прав доступа
(DLTAUTHLR), команда 161, 327, 332

Удалить запись каталога (RMVDIRE),
команда 333

Удалить запись списка библиотек
(RMVLIBLE), команда 218

Удалить запись списка прав доступа
(RMVAUTLE), команда 175, 327

Удалить запись таблицы ключей Kerberos
(RMVKRBKTE), команда
необходимые права доступа к
объектам 450

Удалить контрольные списки
(DLTVLDL) 256

Удалить получатель журнала
(DLTJRNRCV), команда 312

Удалить пользовательский профайл
(DLTUSRPRF), команда
описание 330
пример 127
принадлежность объекта 150

Удалить пользовательский профайл,
меню 127

Удалить пользователя, меню 128

Удалить права доступа к объекту
библиотеки документов (RMVDLOAUT),
команда 332

Удалить список прав доступа (DLTAUTL),
команда 177, 327

Удалить файл кэша идентификационных
данных Kerberos (DLTKRBCCF), команда
необходимые права доступа к
объектам 449

узловой исполнитель в распределенных
системах (QDSNX), пользовательский
профайл 339

управление
доступ
DDM, запрос (DDM) 227
iSeries Access 226
объекты 16
программы системы 16
журнал контроля 310
операции восстановления 228
операции сохранения 228
параметров контроля 69
пользовательский список
библиотек 238
удаленный
вход в систему (системное значение
QRMTSIGN) 35
запуск задания 225

управление (*OBJMGT), права доступа
объекта 138, 360

управление буфером (*SPLCTL),
специальные права доступа
очередь вывода, параметры 224
разрешенные функции 91
риски 91

управление заданиями (*JOBCTL), специальные права доступа
ограничение приоритета (PTYLMT) 100
очередь вывода, параметры 223
разрешенные функции 91
риски 91

управление защитой в Internet (GS), формат файла 651

управление контролем (QAUDCTL), системное значение
обзор 69

Управление контролем (QAUDCTL), системное значение
изменение 334, 751
просмотр 334, 751

управление общей памятью (QSHRMEMCTL), системное значение
возможные значения 38
описание 38

управление объектом (*OBJMGT), уровень контроля 291

управление объектом (OM), тип записи журнала 291

управление системами
изменение
запись журнала контроля (QAUDJRN) 302

управление системами (*SYSMGT), уровень контроля 301

управление сканированием в файловых системах (QSCANFSCCTL), системное значение 36

управление фиксацией
права доступа к объектам, необходимые для применения команд 383

управление шифрами SSL (QSSLCSLCTL), системное значение 44

уровень 10
QSECURITY (уровень защиты), системное значение 12

уровень 20
QSECURITY (уровень защиты), системное значение 12

уровень 30
QSECURITY (уровень защиты), системное значение 13

уровень 40
QSECURITY (уровень защиты), системное значение 14
внутренние управляющие блоки 22

уровень 50
QSECURITY (уровень защиты), системное значение 20
QTEMP (временная), библиотека 21
внутренние управляющие блоки 22
обработка сообщений 21
проверка параметров 18

уровень выгрузки записей контроля (QAUDFRCLVL), системное значение 70, 306

уровень готовности продукта (*PRDAVL), контроль 573

уровень защиты (QSECURITY), системное значение
автоматическое создание пользовательских профайлов 77
введение 2
внутренние управляющие блоки 22
значение, устанавливаемое командой CFGSYSSEC 759
изменение
с уровня 10 на уровень 20 13
с уровня 20 на уровень 30 13
с уровня 20 на уровень 40 19
с уровня 20 на уровень 50 22
с уровня 30 на 20 13
с уровня 30 на уровень 40 19
с уровня 30 на уровень 50 22
с уровня 40 на 20 13
с уровня 40 на уровень 30 20
с уровня 50 на уровень 40 или 30 22

класс пользователя 11
обзор 9
отключение уровня 40 20
отключение уровня 50 22
параметров контроля 272
применение системного значения QLMTSECOFR 213
рекомендации 11
специальные права доступа 11
сравнение уровней 9
уровень 10 12
уровень 20 12
уровень 30 13
уровень 40 14
уровень 50 20
QTEMP (временная), библиотека 21
обзор 20
обработка сообщений 21
проверка параметров 18

уровень контроля (AUDLVL), параметр
*AUTFAIL (ошибка прав доступа), значение 286
*CMD (текст команды), значение 288
*CREATE (создание), значение 288
*DELETE (удаление), значение 288
*JOBDTA (изменение задания), значение 289
*OBJMGT (управление объектом), значение 291
*OFCSRV (функции Office), значение 291
*PGMADP (принятые права доступа), значение 292
*PGMFAIL (сбой программы), значение 292
*SAVRST (сохранение/восстановление), значение 293
*SECURITY (защита), значение 297
*SERVICE (сервисные средства), значение 301
*SPLFDTA (изменения буферного файла), значение 301
*SYSMGT (управление системами), значение 301
изменение 132

уровень контроля (QAUDLVL), системное значение 71
*AUTFAIL (ошибка прав доступа), значение 286
*CREATE (создание), значение 288
*DELETE (удаление), значение 288
*JOBDTA (изменение задания), значение 289
*OBJMGT (управление объектом), значение 291
*OFCSRV (функции Office), значение 291
*PGMADP (принятые права доступа), значение 292
*PGMFAIL (сбой программы), значение 292
*PRTDTA (вывод на принтер), значение 293
*SAVRST (сохранение/восстановление), значение 293
*SECURITY (защита), значение 297
*SERVICE (сервисные средства), значение 301
*SPLFDTA (изменения буферного файла), значение 301
*SYSMGT (управление системами), значение 301
пользовательский профайл 118
просмотр 334, 751
цель 278

уровень контроля за сбоями программ (*PGMFAIL) 292

Уровень пароля (QPWDLVL)
описание 52

Уровень пароля (QPWDLVL), системное значение
описание 52

уровень поддержки
определение 78
основной 78, 85
пользовательский профайл 84
пример изменения 85
промежуточный 78, 85
расширенный 78, 85
сохранен в пользовательском профайле 85

уровень сохранения
число записей контроля 70

установка
операционная система 269

установка лицензионных программ (QLPINSTALL), пользовательский профайл
восстановление 263

установка лицензионных программ, пользовательский профайл (QLPINSTALL)
восстановление 263
значения по умолчанию 339

устройство
виртуальный
автоматическая настройка (системное значение QAUTOVRT) 41
определение 41
защита 211

устройство (продолжение)
права на вход в систему 211
утилита интерактивного определения
данных (IDDU), контроль за
объектом 548
учет ресурсов задания
пользовательский профайл 105

Ф

файл
ведение журнала
инструмент защиты 248
защита
critical 248
записи 248
поля 248
источник
защита 255
описанный в программе
сохранение прав доступа при
удалении 160
планирование защиты 248
права доступа к объектам,
необходимые для применения
команд 404
файл (*FILE), контроль за объектом 550
Файл меню входа в систему 214
файл сообщений
права доступа к объектам,
необходимые для применения
команд 468
файл сообщений (*MSGF), контроль 564
файл, передача
защита 227
файлы jag
файлы классов 255
файлы классов
файлы jag 255
физическая защита 2
параметров контроля 272
планирование 272
фильтр
права доступа к объектам,
необходимые для применения
команд 411
фильтр (*FTR), контроль за
объектом 554
финансовый
права доступа к объектам,
необходимые для применения
команд 412
финансы (QFNC), пользовательский
профайл 339
форма Query Manager (*QMFORM),
контроль 573
формат диаграммы
права доступа к объектам,
необходимые для применения
команд 377
формат диаграммы (*CHTFMT),
контроль 533
формат файла 601
функции Office (*OFCSR), уровень
контроля 291, 542, 562
функция контроля за действиями
CHGSECAUD 308

функция контроля за действиями
(продолжение)
активация 308
завершение 313
функция принятия прав доступа
программой 276
функция создать дамп
*SERVICE, специальные служебные
права доступа 92

Х

хронология, протокол (QHST)
применение для контроля за
защитой 318

Ц

целостность 1
поиск
контроль использования 277
описание 322, 330
целостность объекта
параметров контроля 322
цель
доступность 1
конфиденциальность 1
целостность 1
цифровой ИД
если не найдена частная
идентификация. 121
цифровые подписи
объекта 3
целостность 3
цифровые подписи в системе 3

Ч

частные права доступа
блок-схема 182
восстановление 259, 264
определение 137
планирование приложений 237
права доступа, кэш 207
принадлежность объекта 137
сохранение 259
числовой пароль 80
чтение (*READ), права доступа 138, 360
чтение объекта (ZR), формат файла 743
чтение объекта DLO (YR), формат
файла 739

Ш

шаблон записи (GR), формат файла 639
шаблон имени
пример 170
шифрование
пароль 81

Э

эксперт (*EXPERT), опция
пользователя 112, 113, 114, 167
электронная подпись объекта 3

электронная справочная информация
полноэкранный режим (*HLPFULL,
опция пользователя) 114
эмуляция
права доступа к объектам,
необходимые для применения
команд 392

Я

язык программирования
права доступа к объектам,
необходимые для применения
команд 450



Напечатано в Дании

SC43-0358-10

