IBM

eserver

iSeries

Рекомендации по защите сервера iSeries

Версия 5

SC43-0125-07

IBM

@server

iSeries

Рекомендации по защите сервера iSeries

Версия 5

SC43-0125-07

Примечание

Прежде чем приступить к работе с данной книгой и описанным в ней программным продуктом, обязательно ознакомьтесь с информацией из раздела “Примечания” на стр. 171.

Восьмое издание (апрель 2004 года)

Данное издание относится к версии 5, выпуску 3, модификации 0 IBM Operating System/400 (код продукта 5722-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет явно указано обратное. Данная версия работает не на всех моделях компьютеров с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд CISC.

Настоящее издание заменяет публикацию SC43-0125-05.

Содержание

Рисунки

Таблицы

О книге Рекомендации по защите системы iSeries (SC43-0125-07)

В настоящее время стремительно возрастает роль компьютеров в работе различных организаций. IT-менеджерам, поставщикам программного обеспечения, администраторам по защите и аудиторам приходится пересматривать свое мнение по многим вопросам. Один из таких вопросов - это защита в iSeries.

В системы добавлено много новых функций, значительно отличающихся от стандартных приложений учета ресурсов. Пользователи подключаются к системам разными способами: по локальным сетям, по коммутируемым линиям (удаленный доступ), по беспроводной связи, по сетям различных типов. Часто меню входа в систему пользователям не показывается. Многие организации расширяются до “крупных предприятий” и начинают пользоваться локальными сетями или Internet.

В какой-то момент оказывается, что требуется совершенно новый набор средств для доступа к системе. Системные администраторы и специалисты по защите знают, как защитить информационные ресурсы в столь быстро изменяющихся условиях.

Данная книга содержит практические советы по использованию функций защиты iSeries и созданию необходимых процедур. Приведенные здесь рекомендации рассчитаны на средний уровень защиты системы. Эта информация не содержит полного описания всех существующих функций защиты iSeries. Для того чтобы получить информацию о дополнительных функциях или полную информацию по какой-либо теме, обратитесь к публикациям, перечисленным в разделе Глава 17, “Дополнительная информация”, на стр. 169.

Дополнительно приведена информация о настройке и применении функций защиты, входящих в состав OS/400. В разделах Глава 4, “Настройка системы iSeries для применения средств защиты”, на стр. 29 и “Команды защиты и их меню” на стр. 30 приведена справочная информация о функциях защиты. Эта информация содержит примеры применения функций защиты.

Для кого предназначена эта книга

За защиту системы отвечает **системный администратор** или **администратор защиты**. В их обязанности входит выполнение следующих задач:

- Настройка и управление пользовательскими профайлами
- Настройка системных значений, относящихся к защите
- Управление правами доступа к объектам
- Разработка и отслеживание стратегий защиты

Эта информация предназначена для тех пользователей, которые отвечают за настройку защиты одной или нескольких систем iSeries. При этом предполагается, что:

- Вы знакомы с основными процедурами работы с iSeries, такими как вход в систему и применение команд.
- Вам известны основные элементы защиты iSeries: уровни защиты, необходимые системные значения, пользовательские профайлы и способы защиты объектов.

Примечание: В разделе Глава 1, “Основные элементы защиты iSeries”, на стр. 3 приведен обзор этих элементов. Если основные элементы вам известны, то ознакомьтесь с разделом *Основы защиты и планирования* в iSeries Information Center. Дополнительная информация приведена в разделе “Необходимая и полезная информация”.

- Вы активизировали защиту в системе, установив системное значение уровня защиты (QSECURITY) равным 30 или выше.

Фирма IBM постоянно расширяет возможности защиты в iSeries. Все изменения отражаются в совокупном пакете исправлений, соответствующем установленному у вас выпуску системы. Регулярно проверяйте наличие в нем PTF, относящихся к защите.

Как работать с этой книгой

Если функции защиты не настроены в системе, либо в системе установлен продукт Security ToolKit for OS/400 более раннего выпуска, выполните следующие действия:

1. Прежде всего ознакомьтесь с разделом Глава 2, “Мастер настройки защиты и планировщик конфигурации защиты iSeries”, на стр. 11. В нем описаны программы, позволяющие выбрать рекомендуемые средства защиты и начать работу с ними.
2. Общая информация о защите приведена в справочнике Security Reference, электронную версию которого можно найти в iSeries Information Center.

Примечание

В данном документе приведено *много* советов по организации защиты iSeries. В вашей системе могут потребоваться только некоторые функции защиты. С помощью этого документа можно получить общее представление о возможных способах взлома системы и способах защиты от взлома. После этого вы сможете уделить особое внимание областям, наиболее важным для вашей системы.

Необходимая и полезная информация

Отправной точкой при поиске технической информации об iSeries может служить справочная система iSeries Information Center.

Информацию Information Center можно получить двумя способами:

- С Web-сайта

  `http://www.ibm.com/eserver/iseries/infocenter`
- С компакт-диска *iSeries Information Center*, SK3T-4091-04. Этот компакт-диск поставляется вместе с аппаратным обеспечением новых систем iSeries и с заказами на обновление программного обеспечения IBM Operating System/400. Вы также можете заказать этот компакт-диск с помощью IBM Publications Center:

  `http://www.ibm.com/shop/publications/order`

Справочная система iSeries Information Center содержит информацию по таким вопросам, как установка программного и аппаратного обеспечение, применение Linux, WebSphere, Java, средств обеспечения высокой готовности, баз данных, логических разделов, команд CL и системных интерфейсов прикладных программ (API). Кроме того, в состав этой справочной системы входят мастера и советники,

которые помогут вам при планировании, устранении неполадок, а также при настройке аппаратного и программного обеспечения iSeries.

С каждым заказом на аппаратное обеспечение поставляется компакт-диск *iSeries Setup and Operations CD-ROM*, SK3T-4098-02. Этот компакт-диск содержит продукт IBM @server IBM e(logo)server iSeries Access for Windows и мастера EZ-Setup. Семейство продуктов iSeries Access Family предоставляет широкий набор функций клиента и сервера для подключения PC к серверам iSeries. Мастер EZ-Setup позволяет автоматизировать выполнение многих задач по настройке iSeries.

Ждем ваших отзывов

Фирма IBM будет признательна вам за ваши отзывы и комментарии, поскольку они позволят повысить точность и качество предоставляемой информации. Если у вас есть замечания по этой книге или другой документации iSeries, заполните форму для отзывов читателей в конце книги.

- Вы можете отправить отзывы по обычной почте - адрес напечатан на обратной стороне формы для отзывов. Если вы находитесь за пределами США, вы можете передать форму в местное представительство IBM для ее отправки за счет адресата.
- Ниже приведены номера телефонов для отправки отзывов по факсимильной связи:
  - Для США, Канады и Пуэрто-Рико: 1-800-937-3430
  - Для других стран: 1-507-253-5192
- Если вы предпочитаете отправить сообщение по электронной почте, то воспользуйтесь одним из следующих адресов:
  - Комментарии по книгам:

    RCHCLERK@us.ibm.com
  - Комментарии по iSeries Information Center:

    RCHINFOC@us.ibm.com

Обязательно укажите следующую информацию:

- Название книги или раздела iSeries Information Center.
- Идентификатор книги.
- Номер страницы или название раздела, к которому относятся комментарии.

Часть 1. Основные функции защиты iSeries

Глава 1. Основные элементы защиты iSeries

В этом разделе приведен краткий обзор основных элементов, в совокупности своей обеспечивающих защиту системы iSeries. В других разделах данной книги будет дана дополнительная информация, например, советы по использованию этих основных элементов и выбор наиболее подходящей для вашей организации конфигурации защиты.

Уровни защиты

С помощью системного значения Уровень защиты (QSECURITY) вы можете задать степень защищенности вашей системы. Можно выбрать один из пяти уровней:

Уровень 10:

Защита в системе не установлена. Для работы с системой пароль не требуется. Если указанный при входе в систему пользовательский профайл не существует, он автоматически создается.

ВНИМАНИЕ:

Начиная с версии V4R3, значение 10 для QSECURITY недопустимо. Если в системе установлен уровень защиты 10, то при установке версии 4 выпуска 3 это значение сохранится. Но если вы измените его на любое другое значение, то вернуть обратно уровень 10 уже не удастся. Фирма IBM Corporation не рекомендует устанавливать уровень защиты 10, так как он не обеспечивает безопасность системы. Фирма **IBM не предоставляет услуги по устранению неполадок, возникших на уровне защиты 10 и невозможных на более высоких уровнях защиты.**

Уровень 20:

Для входа в систему требуется указать ИД пользователя и пароль. Уровень защиты 20 часто называется **защита входа в систему**.По умолчанию у всех пользователей есть права доступа *ALLOBJ, что означает, что у них есть доступ ко всем объектам.

Уровень 30:

Для входа в систему требуется указать ИД пользователя и пароль. Для работы с объектами пользователю необходимо предоставить права доступа к ним, так как по умолчанию эти права не предоставляются. Этот уровень защиты называется **защита ресурсов**.

Уровень 40:

Для входа в систему требуется указать ИД пользователя и пароль. Помимо защиты ресурсов в системе доступны функции **защиты целостности данных**. Эти функции, включающие в себя проверку параметров интерфейсов операционной системы, обеспечивают защиту системы и ее объектов от их изменения пользователями. В большинстве случаев для системы рекомендуется уровень защиты 40. Новая система iSeries с операционной системой выпуска V4R5 или более позднего выпуска поставляется с уровнем защиты 40.

Уровень 50:

Для входа в систему требуется указать ИД пользователя и пароль. В системе

установлена защита ресурсов и целостности данных системы уровня 40,а также применяется **расширенная защита целостности данных**, в том числе ограничение на обмен сообщениями между программами режима системы и программами режима пользователя. Уровень защиты 50 предназначен для систем iSeries с повышенными требованиями к защите.

Примечание: Уровень 50 обязателен для сертификации C2 (и сертификации FIPS-140).

В главе 2 книги *iSeries Security Reference* содержится дополнительная информация об уровнях защиты и об изменении уровня защиты системы.

Глобальные параметры

Глобальные параметры системы определяют ваши возможности при работе в системе, а также степень доступности системы другим пользователям. Эти параметры включают:

Системные значения защиты:

Эти системные значения служат для управления защитой системы. Они поделены на четыре группы:

- Основные системные значения защиты
- Прочие системные значения защиты
- Системные значения управления паролями
- Системные значения управления контролем

Предназначению отдельных системных значений посвящено несколько разделов этой книги. В главе 3 книги *iSeries Security Reference* описаны все системные значения, определяющие защиту системы.

Сетевые атрибуты:

Сетевые атрибуты управляют ролью вашей системы в сети, объединяющей ее с другими компьютерами. Подробная информация о сетевых атрибутах приведена в книге *Work Management*.

Описание подсистем и другие элементы управления работой:

Элементы управления работой определяют возможности и среду вашей работы в системе. Предназначению некоторых значений управления работой посвящено несколько разделов этого документа. Полная информация приведена в книге *Work Management*.

Конфигурация средств связи:

Конфигурация средств связи также влияет на ваши возможности при работе с системой. В некоторых разделах этого документа предложены рекомендации по организации защиты системы, подключенной к сети.

Пользовательские профайлы

Для каждого пользователя в системе **должен быть** определен пользовательский профайл. Пользователь может войти в систему только тогда, когда для него создан профайл. Пользовательские профайлы позволяют управлять доступом к сервисным средствам, таким как DASD и функция создания дампа оперативной памяти. Дополнительная информация приведена в разделе “Применение сервисных средств” на стр. 64.

Пользовательский профайл - это мощное и гибкое средство работы. В нем определяются возможности пользователя и задается степень доступности системы. Все параметры пользовательского профайла описаны в книге *iSeries Security Reference*.

Профайлы групп

Профайл группы - это особый тип пользовательского профайла. Если требуется задать одинаковые права доступа нескольким пользователям, с помощью профайла группы вы можете сделать это за один прием. На основе профайла группы можно создать пользовательский профайл. Для этого нужно скопировать профайл группы, либо изменить права доступа пользователя в меню стратегий защиты программы Навигатор iSeries.

Главы 5 и 7 книги *iSeries Security Reference* предоставляют дополнительную информацию о планировании и применении профайлов групп.

Защита ресурсов

Защита ресурсов позволяет задать пользователей, которым разрешен доступ к объектам, и их возможности при работе с этими объектами. Разрешение на работу с объектом называется **правами доступа**. При задании прав доступа к объектам необходимо следить, чтобы у пользователей было достаточно прав для выполнения их работы, но чтобы они при этом не могли исследовать систему и изменять ее критические параметры. Права доступа к объекту предоставляют пользователю возможность работать с данным объектом и определяют набор операций, которые разрешено выполнять над объектом. С применением специальных уточненных пользовательских прав доступа обращение к ресурсу объекта может быть ограничено добавлением или изменением записей. С помощью системных ресурсов пользователю может быть предоставлен доступ к специальным системным подмножествам прав доступа: *ALL, *CHANGE, *USE и *EXCLUDE.

Чаще всего защиту ресурсов устанавливают для файлов, программ, библиотек и каталогов, но вы можете определить права доступа к любому отдельному объекту системы.

В разделе Глава 5, “Защита информации и права доступа к объектам” обсуждается важность применения прав доступа в вашей системе. В главе 5 книги *iSeries Security Reference* описаны опции настройки защиты ресурсов.

Ограничение доступа к функции программы

Ограничение доступа к функции программы позволяет обеспечить защиту программы в том случае, если в системе iSeries нет объекта программы, доступ к которому можно было бы запретить. До того как в версии V4R3 была добавлена поддержка защиты функций программ, аналогичного эффекта можно было добиться, создав список прав доступа или другой объект и управлять доступом к функции программы с помощью прав доступа к этому объекту. Теперь вы можете ограничивать доступ к функции программы, что упрощает управление доступом к приложению, к элементам приложения или к функциям программ.

В Навигаторе iSeries предусмотрено два способа управления доступом пользователей к функциям приложений. Первый способ подразумевает использование поддержки Администрирования приложений:

1. Щелкните правой кнопкой мыши на значке системы, к функциям которой нужно ограничить доступ.
2. Выберите пункт **Администрирование приложений**.
3. Если вы работаете в административной системе, выберите пункт **Локальные параметры**. В противном случае, перейдите к следующему шагу.
4. Выберите функцию.
5. Выберите **Разрешать доступ по умолчанию**, если это необходимо. Эта опция указывает, что по умолчанию всем пользователям будет разрешено работать с функцией.
6. Выберите значение **Доступ ко всем объектам**, если это необходимо. Эта опция разрешает работать с функцией всем пользователям, у которых есть права доступа ко всем объектам.
7. Выберите опцию **Настроить**, если это необходимо. С помощью кнопок **Добавить** и **Удалить** измените списки пользователей и групп под заголовками **Доступ разрешен** и **Доступ запрещен** в окне **Настроить права доступа**.
8. При необходимости выберите опцию **Отменить настройку**. Будут удалены все права доступа, настроенные для выбранной функции.
9. Нажмите кнопку **OK** и закройте окно **Администрирование приложений**.

Второй способ управления доступом пользователей заключается в использовании списка Пользователи и группы программы Навигатор iSeries:

1. В окне программы Навигатор iSeries разверните список **Пользователи и группы**.
2. Выберите опцию **Все группы**, **Группы** или **Пользователи, не входящие в группу**. Появится список пользователей и групп.
3. Щелкните правой кнопкой мыши на имени пользователя или группы и выберите пункт **Свойства**.
4. Выберите опцию **Возможности**.
5. Перейдите на страницу **Приложения**.
6. Измените на этой странице права доступа пользователя или группы.
7. Дважды нажмите кнопку **OK**, чтобы закрыть окно **Свойства**.

Более подробная информация о функциях защиты Навигатора iSeries приведена в разделе “Функции защиты Навигатора iSeries” на стр. 158.

Если вы - разработчик приложения, то вы можете с помощью API ограничения доступа к программным функциям выполнять следующее:

- Регистрировать функцию
- Получать информацию о функции
- Задать пользователей, которые могут применять эту функцию
- Проверять, разрешено ли конкретному пользователю работать с функцией

Примечание: Эта поддержка **не** может считаться заменой защите ресурсов. Ограничение доступа к программным функциям не может запретить доступ пользователя к ресурсу (например, к файлу или программе) из другого интерфейса.

Для использования этой поддержки в приложении поставщик приложения должен при установке приложения зарегистрировать функции. Зарегистрированная функция соответствует блоку кода конкретной функции в приложении. При запуске приложения пользователем до вызова этого блока кода вызывается API. Этот API вызывает API проверки уровня доступа для того, чтобы проверить, разрешено ли

пользователю работать с функцией. Если соответствующее разрешение есть, то запускается блок кода. В противном случае код блока не запускается.

Примечание: API записывает в базу данных регистрации (WRKREGINF) ИД функции длиной 30 символов. Хотя точек выхода, связанных с ИД функций, применяемыми API ограничения доступа к функциям, не предусмотрено, их наличие обязательно. Для регистрации в реестре **необходимо** указать имя в формате точки выхода. Для этого API Зарегистрировать функцию создает фиктивное имя формата и использует его при регистрации всех функций. Для фиктивного имени программа точки выхода не вызывается.

Системный администратор указывает, каким пользователям разрешен доступ к функции, а каким запрещен. Для управления доступом к функции программы может применяться API или функция Администрирование приложений программы Навигатор iSeries. Информация об API ограничения доступа к функциям программ приведена в книге *iSeries server API Reference*. Дополнительные сведения об управлении доступом к функциям приведены в разделе “Функции защиты Навигатора iSeries” на стр. 158.

Контроль за действиями

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. Обычно администратор защиты выполняет соответствующие действия регулярно. 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 безопасность 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 своевременного их аннулирования
  - Установка новых продуктов
- Для подготовки к выполнению определенной операции: установке нового приложения, повышению уровня защиты или настройке новой сети.

В этом разделе описаны рекомендуемые действия для любой из перечисленных ситуаций. Выбор объектов для контроля и частота его проведения зависят от размера организации и требований к защите.

Контроль за действиями предполагает вызов команд, а также просмотр протокола и журнала. Для пользователя, контролирующего действия, можно создать отдельный пользовательский профайл. Такому профайлу должны быть предоставлены особые права доступа *AUDIT, необходимые для изменения параметров контроля в системе. Для выполнения некоторых задач контроля, описанных в этой главе, необходим пользовательский профайл со специальными правами доступа *ALLOBJ и *SECADM. По истечении периода контроля пароль пользовательского профайла, применяемого для контроля за действиями, следует изменить на *NONE.

Дополнительная информация о контроле за действиями приведена в главе 9 книги *Security Reference*.

Пример: Отчет о системных атрибутах защиты

рис. 1 содержит пример вывода команды Печать системных атрибутов защиты (PRTSYSSECA). Отчет содержит системные значения, влияющие на защиту, и сетевые атрибуты, рекомендуемые для систем с обычными требованиями к защите. В нем показана также текущая конфигурация системы.

Примечание: В столбце отчета *Текущее значение* указаны текущие значения параметров системы. Сравните рекомендуемую и текущую конфигурации; это поможет вам определить недостатки в защите системы.

```
Системные атрибуты защиты

Системное значение
Имя              Текущее значение       Рекомендуемое значение
QALWOBJRST       *NONE                  *NONE
QALWUSRDMN       *ALL                   QTEMP
QATNPGM          QEZMAIN   QSYS         *NONE
QAUDENDACN       *NOTIFY                *NOTIFY
QAUDFRCLVL       *SYS                   *SYS
QAUDCTL          *AUDLVL                *AUDLVL   *OBJAUD
QAUDLVL          *SECURITY              *AUTFAIL  *CREATE
                                        *DELETE   *SECURITY
                                        *SAVRST   *NOQTEMP
```

Рисунок 1. Отчет о системных атрибутах защиты - Пример (Часть 1 из 4)

```
QAUTOCFG         0                      0
QAUTORMT         1                      0
QAUTOVRT         9999                   0
QCMNRCYLMT       0 0                    0 0
QCRTAUT          *CHANGE                Управление на уровне библиотеки
QCRTOBJAUD       *NONE                  Управление на уровне библиотеки
QDEVRCYACN       *DSCMSG                *DSCMSG
QDSCJOBITV       120                    120
QDSPSGNINF       1                      1
QINACTITV        60                     60
QINACTMSGQ       *ENDJOB                *ENDJOB
QLMTDEVSSN       0                      1
QLMTSECOFR       0                      1
QMAXSGNACN       2                      3
QMAXSIGN         3                      3
```

Рисунок 1. Отчет о системных атрибутах защиты - Пример (Часть 2 из 4)

```
QPWDEXPITV      60                  60
QPWDLMTAJC      1                   1
QPWDLMTCHR      *NONE               AEIOU@$#
QPWDLMTREP      1                   2
QPWDLVL         0
QPWDMAXLEN      8                   8
QPWDMINLEN      6                   6
QPWDPOSDIF      1                   1
QPWDRQDDGT      1                   1
QPWDRQDDIF      0                   1
QPWDVLDPGM      *NONE               *NONE
QRETSVRSEC      0                   0
QRMTIPL         0                   0
QRMTSIGN        *FRCSIGNON          *FRCSIGNON
QSECURITY       50                  50
QSHRMEMCTL      1                   0
QSRVDMP         *DMPUSRJOB          *NONE
QUSEADPAUT      *NONE               CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                    CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                    CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST      1                   3
```

Рисунок 1. Отчет о системных атрибутах защиты - Пример (Часть 3 из 4)

```
Системные атрибуты защиты

Сетевой атрибут
Имя             Текущее значение    Рекомендуемое значение
DDMACC          *OBJAUT             *REJECT
JOBACN          *FILE               *REJECT
PCSACC          *OBJAUT             *REJECT
```

Рисунок 1. Отчет о системных атрибутах защиты - Пример (Часть 4 из 4)

Глава 2. Мастер настройки защиты и планировщик конфигурации защиты iSeries

Мастер настройки защиты iSeries и планировщик конфигурации защиты eServer помогут вам выбрать значения для параметров защиты сервера. Мастер настройки защиты iSeries можно запустить из программы Навигатор iSeries/ Он создает отчет с описанием рекомендуемой стратегии защиты на основе информации, полученной от пользователя. В дальнейшем вы сможете применить этот отчет при настройке защиты вашей системы.

Мастер настройки защиты iSeries и планировщик конфигурации защиты eServer помогут вам спланировать и реализовать основную стратегию защиты сервера iSeries. Эти программы значительно упрощают настройку защиты в системе. Мастер задает пользователю ряд общих вопросов о конфигурации сервера и на основании полученных ответов создает рекомендации по настройке защиты в системе. При необходимости можно автоматически применить рекомендуемую стратегию защиты системы. Мастер входит в состав операционной системы OS/400.

Планировщик конфигурации защиты eServer - это версия Мастера настройки защиты, работающая в режиме Web. Эта программа позволяет выбирать опции, отвечающие вашим потребностям в защите, и выдает отчет с предложениями функций, требуемых для защиты вашей системы.

Планировщик конфигурации защиты eServer - это версия мастера настройки защиты с Web-интерфейсом. Как и мастер, он предлагает ряд рекомендаций по реализации защиты в системе. Однако советник не позволяет автоматически применить эти рекомендации. На основании информации, полученной от пользователя, он создает список системных значений защиты и других атрибутов, которые можно установить в системе.

Мастер настройки защиты

Выбрать правильные значения для параметров защиты iSeries достаточно сложно. Если вы впервые разрабатываете стратегию защиты сервера iSeries, либо рабочая среда iSeries была недавно изменена, воспользуйтесь Мастером настройки защиты.

Для чего нужен мастер?

- Программа-мастер - это средства, разработанное для того, чтобы помочь неопытным пользователям при установке или настройке компонентов системы.
- Мастер запрашивает у пользователя необходимую информацию. В зависимости от ответов изменяется набор задаваемых вопросов.
- После того как пользователь ответит на все вопросы Мастера, на экране появится последнее окно диалога. Для установки и настройки компонента пользователю нужно будет нажать кнопку **Готово**.

Задачи Мастера настройки защиты

Задача Мастера настройки защиты заключается в том, чтобы настроить перечисленные ниже параметры исходя из информации, полученной от пользователя.

- Системные значения и сетевые атрибуты, связанные с защитой системы.
- Параметры создания отчетов для контроля за защитой системы.

- Кроме того, мастер создает отчет с информацией для администратора и отчет с информацией для пользователя:
  - Отчет с информацией для администратора содержит сведения о рекомендуемых параметрах защиты и о всех процедурах, которые необходимо выполнить до их настройки.
  - Отчет с информацией для пользователя содержит сведения для стратегии защиты бизнеса. Например, в этот отчет включены правила составления паролей.
- Мастер предлагает рекомендуемые значения для многих параметров защиты системы.

Задачи Мастера настройки защиты

- Ниже перечислены задачи Мастера настройки защиты:
  - Определить необходимые для защиты системы параметры, основываясь на ответах пользователя и в соответствующий момент установить эти параметры.
  - Создать подробные отчеты, в которые будет включена следующая информация:
    - Отчет с объяснениями рекомендаций Мастера.
    - Отчет с подробным описанием процедур, которые должны быть выполнены перед окончательной настройкой защиты.
    - Отчет с необходимой связанной информацией, который будет распространена между пользователями системы.
- Эти элементы задают основную стратегию защиты, которая будет действовать в вашей системе.
- Программа-мастер укажет также отчеты журнала по контролю, для которых нужно будет запланировать периодический запуск. Будучи запланированными, эти отчеты выполняют следующее:
  - Контролируют соблюдение стратегии защиты.
  - Проверяют, что все изменения стратегий защиты выполнялись исключительно с вашего разрешения.
  - Планируют отчеты отслеживания событий защиты в вашей системе.
- Вы можете сохранить рекомендации программы-мастера или применить некоторые из них в вашей системе.

Примечание: В одной системе Мастер настройки защиты можно запускать несколько раз, например, для того, чтобы пользователи могли просмотреть параметры ранее установленной защиты. Мастер настройки защиты предусмотрен в системах выпуска V3R7 и более поздних выпусков (во всех системах, поддерживающих Навигатор iSeries).

Для работы с Навигатором iSeries на персональном компьютере с операционной системой Windows 95/NT должен быть установлен продукт IBM iSeries Access для Windows и настроено соединение с сервером iSeries. Во время работы с мастером соединение с iSeries должно быть активно. Пользователь должен обладать специальными правами доступа *ALLOBJ, *SECADM, *AUDIT и *IOSYSCFG. Информация о подключении персонального компьютера с операционной системой Windows 95/NT к системе iSeries приведена в разделе IBM iSeries Access для Windows справочной системы Information Center (более подробные сведения можно найти в разделе “Необходимая и полезная информация” на стр. xii).

Для запуска Мастера настройки защиты выполните следующие действия:

1. В окне Навигатора iSeries разверните значок своего сервера.
2. Щелкните правой кнопкой мыши на опции **Защита** и выберите пункт **Настроить**.
   - При выборе опции **Защита** в программе Навигатор iSeries на сервер iSeries отправляется запрос о специальных правах доступа, предоставленных пользователю.

- Если окажется, что пользователь не обладает какими-либо из требуемых специальных прав доступа (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM), опция **Настроить** показана не будет и вызвать Мастер по настройке защиты не удастся.

3. В предположении, что у пользователя есть все необходимые права доступа:
   - Будут восстановлены предыдущие ответы программы-мастера.
   - Будет получена информация о текущих параметрах защиты.

Мастер выдаст одно из трех окон приветствия, выбор которого определяется следующими условиями:

- Программа-мастер не вызывалась ранее для целевого сервера iSeries.
- Программа-мастер вызывалась ранее, но изменения в настройке защиты не были приведены в действие.
- Программа-мастер вызывалась ранее и изменения в настройке защиты вступили в силу.

Информацию о планировании конфигурации защиты можно получить и без помощи программы Навигатор iSeries. Планировщик конфигурации защиты eServer - это версия Мастера по настройке защиты, предназначенная для работы в Web и имеющая одно отличие. Советник по настройке защиты не выполняет автоматическую настройку. Она запрашивает у пользователя информацию и в зависимости от полученных ответов выдает отчет с рекомендациями по параметрам защиты. Обратиться к планировщику конфигурации защиты eServer можно с помощью eServer Information Center:

`http://publib.boulder.ibm.com/eserver/`

Планировщик конфигурации защиты eServer

Планировщик конфигурации защиты eServer - это версия Мастера настройки защиты, работающая в режиме Web. Она задает пользователю те же вопросы, что и Мастер, и также в зависимости от ответов выдает рекомендации. Основные различия этих двух программ заключаются в следующем:

- Планировщик конфигурации защиты eServer **не выполняет** следующие действия:
  - Создание отчетов.
  - Сравнение текущей конфигурации с рекомендуемой.
  - Автоматическое изменение системных значений.
- Рекомендации планировщика конфигурации защиты eServer нельзя автоматически применить в системе.

Планировщик конфигурации защиты eServer создает программный код на CL, который можно скопировать, отредактировать и применить для автоматической настройки защиты. Кроме того, планировщик конфигурации защиты eServer содержит ссылку на документацию по серверу iSeries. В ней вы можете найти сведения о конкретном системном значении или отчет, которые помогут вам определить, насколько данная установка подходит для вашей среды.

Для обращения к планировщику конфигурации защиты eServer укажите в вашем браузере Internet следующий адрес:

`http://publib.boulder.ibm.com/eserver/`

Глава 3. Управление входом в систему через меню

Если вы решили установить ограничения на вход в вашу систему, то, очевидно, начать следует с меню Вход в систему. Ниже перечислены функции, с помощью которых можно ограничить вход в систему через это меню.

Правила выбора паролей

Для того чтобы ограничить вход в систему, выполните следующие действия:
- Задайте стратегию, требующую, чтобы пароли были уникальными и сложными.
- Задайте системные значения, которые будут обеспечивать выполнение этих правил. В Табл. 1 перечислены рекомендуемые системные значения.

Сочетание требований, приведенных в Табл. 1, задает строгие ограничения на составление паролей, исключая тем самым возможность случайного угадывания пароля, присутствующую при задании простых паролей. Пользователю может быть сложно придумать пароль, который отвечает всем этим требованиям.

Предоставьте пользователям следующую информацию:
1. Список критериев для задания паролей.
2. Примеры допустимых и недопустимых паролей.
3. Подсказки для составления подходящего пароля.

С помощью команды Настроить защиту системы (CFGSYSSEC) можно задать эти значения. С помощью команды Печать атрибутов защиты системы (PRTSYSSECA) можно напечатать текущие системные значения.

Раздел 3 книги *iSeries Security Reference*. Подробная информация о команде CFGSYSSEC приведена в разделе “Значения, устанавливаемые командой Настроить защиту системы” на стр. 39.

Таблица 1. Системные значения установки пароля

Имя системного значения	Описание	Рекомендуемое значение
QPWDEXPITV	Как часто пользователи должны менять свой пароль. Для отдельных пользователей можно задать различные значения.	60 (дней)
QPWDLMTAJC	Запрещено ли в пароле совпадение соседних символов.	1 (да)
QPWDLMTCHR	Символы, недопустимые в паролях. [2]	AEIOU#$@
QPWDLMTREP	Запрещен ли в пароле повтор символов.	2 (не разрешен повтор соседних символов)
QPWDLVL	Определяет максимально допустимую длину пользовательского пароля - 10 или 128 символов.	0[3]
QPWDMAXLEN	Максимальное число символов в пароле.	8
QPWDMINLEN	Минимальное число символов в пароле.	6
QPWDPOSDIF	Должен ли каждый символ пароля отличаться от символа, стоявшего в той же позиции в предыдущем пароле.	1 (да)
QPWDRQDDGT	Должна ли присутствовать в пароле хотя бы одна цифра.	1 (да)
QPWDRQDDIF	Период, после которого пользователь может повторно указать данный пароль.[2]	5 или меньше (сроков действия)[1]
QPWDVLDPGM	Какая программа выхода вызывается для проверки назначенного пароля.	*NONE

Таблица 1. Системные значения установки пароля (продолжение)

Имя системного значения	Описание	Рекомендуемое значение

Примечания:

1. Системное значение QPWDEXPITV задает период действия пароля, например, 60 дней, по истечении которого пароль необходимо сменить. Этот период называется **сроком действия пароля**. Системное значение QPWDRQDDIF задает, через сколько таких периодов можно снова выбрать этот пароль. В Главе 3 книги *iSeries Security Reference* приведена подробная информация о совместном применении всех этих системных значениях.
2. Значение QPWDLMTCHR не может использоваться с паролями уровней 2 и 3. Дополнительная информация приведена в разделе “Уровни паролей”.
3. Дополнительная информация о выборе уровня пароля приведена в разделе “Планирование изменения уровня пароля” на стр. 17.

Уровни паролей

Начиная с выпуска V5R1, системное значение QPWDLVL можно настроить на применение более надежных паролей. В предыдущих выпусках пользователи могли указывать пароли не длиннее 10 символов, причем некоторые символы не допускались. Теперь пользователи могут задать пароль (или пароль-предложение) длиной до 128 символов, в зависимости от установленного уровня паролей. Существуют следующие уровни паролей:

- **Уровень 0:** Уровень, применяемый в системе по умолчанию. Пароли уровня 0 могут состоять не более чем из 10 символов и содержать только символы A-Z, 0–9, #, @, $ и _. Пароли уровня 0 являются наименее защищенными.
- **Уровень 1:** Пароли соответствуют тем же требованиям, что и на уровне 0, однако пароли Поддержки сетевого окружения Windows в iSeries (далее именуемой iSeries NetServer) не сохраняются.
- **Уровень 2:** На этом уровне применяются надежные пароли. Такой уровень можно установить на время тестирования. Пароли сохраняются для пользователей уровня 0 или 1, если их длина не превышает 10 символов, и в них входят только символы из набора уровня 0 или 1. На этом уровне пароли (или пароли-предложения) отвечают следующим требованиям:
  - Длина пароля - 128 символов.
  - В паролях допускаются любые символы.
  - Пароли не могут состоять только из пробелов; конечные пробелы удаляются.
  - В паролях учитывается регистр символов.
- **Уровень 3:** На этом уровне применяются самые надежные пароли и самые сложные алгоритмы шифрования. Характеристики паролей этого уровня совпадают с характеристиками паролей уровня 2. Пароли этого уровня для iSeries NetServer не сохраняются.

Пароль уровня 2 или 3 можно указать лишь в том случае, если все системы, подключенные к сети, отвечают следующим требованиям:

- Установлена операционная система выпуска V5R1 или выше
- Уровень паролей равен 2 или 3

Аналогично, при входе в систему пользователи должны применять пароли одного уровня. Уровень пароля устанавливается для всей системы; его нельзя изменить для отдельного пользователя.

Планирование изменения уровня пароля

К изменению уровня пароля следует отнестись с особой тщательностью. Необдуманное изменение уровня пароля может привести к сбоям при взаимодействии с другими системами или к невозможности входа пользователей в систему. Перед изменением системного значения QPWDLVL убедитесь в том, что вы сохранили данные о защите системы с помощью команды SAVSECDTA или SAVSYS. При наличии резервной копии текущей системы вы сможете сбросить пароли для всех пользовательских профайлов, если вам потребуется вернуться на более низкий уровень паролей.

В работе продуктов системы и ее клиентов могут возникать ошибки, если системное значение Уровень паролей (QPWDLVL) равно 2 или 3. Все продукты и клиенты, отправляющие пароли системе в зашифрованном виде, необходимо обновить в соответствии с новыми 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 новый алгоритм шифрования, не будет принят сервером, даже если он содержит только допустимые символы. Это относится и к обмену данными между двумя равноправными узлами iSeries, в ходе которого для идентификации систем iSeries применяются зашифрованные значения.

Несовместимость паролей разных уровней влияет и на работу тех продуктов, которые служат для создания других программ (например, Java Toolbox). Продукты других фирм, использующие такое программное обеспечение предыдущих версий, будут работать правильно только после его обновления.

В силу вышесказанного становится понятно, почему изменять уровень паролей следует с особой осторожностью.

Изменение значения QPWDLVL с 0 на 1

Если в системе применяются пароли уровня 1, и система не обменивается данными с продуктом Поддержка сетевого окружения Windows 95/98/ME в AS/400 (iSeries NetServer), то пароли iSeries NetServer можно удалить из системы. Удаление неиспользуемых зашифрованных паролей позволит повысить общую защищенность системы.

Если системное значение QPWDLVL 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 iSeries NetServer.

Изменение значения QPWDLVL с 0 или 1 на 2

В паролях уровня 2 учитывается регистр и они могут содержать до 128 символов (такие пароли также называются паролями-предложениями); процедура возврата с этого уровня на уровень 0 или 1 максимально упрощена.

Независимо от уровня паролей системы, пароли уровня 2 и 3 создаются при каждом изменении пароля или входе пользователя в систему. Создание паролей уровня 2 и 3, когда в системе применяются пароли уровня 0 или 1, позволяет подготовить систему к переходу к паролям уровня 2 или 3.

Перед тем как присвоить параметру QPWDLVL значение 2, необходимо найти все пользовательские профайлы, пароли которых не соответствуют требованиям уровня 2. Для этого можно вызвать команду DSPAUTUSR или PRTUSRPRF

TYPE(*PWDINFO). После этого в найденные профайлы нужно добавить пароли уровня 2 или 3 одним из следующих способов.

- Изменить пароль пользовательского профайла с помощью команды CL CHGUSRPRF или CHGPWD или API QSYCHGPW. При этом будет изменен пароль уровня 0 или 1; будут также созданы два эквивалентных пароля уровней 2 и 3 с учетом регистра символов. Это будут версии паролей уровня 2 или 3 в верхнем и в нижнем регистре.

  Например, при изменении пароля на 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 введен верно и в пользовательском профайле нет пароля уровня 2 или 3, то система создаст два эквивалентных пароля уровня 2 и 3 с учетом регистра символов. Это будут версии паролей уровня 2 или 3 в верхнем и в нижнем регистре.

Если в профайле нет пароля уровня 0 или 1 или если пользователь попытается войти в систему с помощью продукта, применяющего подстановку паролей, то отсутствие при этом в профайле пароля уровня 2 или 3 может стать причиной неполадки. В этих случаях при установке уровня паролей 2 пользователь не сможет войти в систему.

Если в пользовательском профайле нет пароля уровня 2 или 3, в пользовательском профайле нет пароля уровня 0 или 1 и пользователь пытается войти в систему с помощью продукта, не шифрующего пароли, то система предоставляет пользователю доступ на уровне паролей 0 и создает для пользовательского профайла два пароля уровня 2, так как описано выше. При последующих входах в систему пользователю будет предоставляться доступ на уровне паролей 2.

Если какие-либо клиенты или службы не были обновлены для применения нового алгоритма подстановки паролей (паролей-предложений), то на уровне паролей QPWDLVL 2 такие клиенты и службы будут работать неправильно. Администратор должен убедиться в том, что клиент или служба были обновлены для применения нужного алгоритма подстановки паролей.

К числу клиентов и служб, использующих подстановку паролей, относятся:

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- Функция печати iSeries NetServer
- DDM
- DRDA
- SNA LU6.2

Перед установкой в системе уровня паролей 2 настоятельно рекомендуется сохранить все данные о защите. При необходимости это может существенно упростить обратный переход к уровню QPWDLVL 0 или 1.

Остальные системные значения паролей, такие как QPWDMINLEN и QPWDMAXLEN, следует изменять только после проверки работы системы с системным значением QPWDLVL 2. При необходимости это существенно упростит обратный переход к уровню QPWDLVL 0 или 1. Однако учтите, что системному значению QPWDLVL можно присвоить 2, только если системное значение QPWDVLDPGM равно *REGFAC или *NONE. Таким образом, если вы применяете программу проверки

паролей, то вы можете создать ее новую версию, которую можно будет зарегистрировать для точки выхода QIBM_QSY_VLD_PASSWRD с помощью команды ADDEXITPGM.

На уровне 2 поддерживаются пароли iSeries NetServer, поэтому все функции и службы, применяющие эти пароли, 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 указании паролей длиннее 10 символов пароль уровня 0 или 1 удаляется. При возврате к уровню паролей 0 или 1 войти в систему под управлением соответствующего профайла будет невозможно.
- Если пароли содержат специальные символы или не соответствуют правилам составления простых имен объектов (за исключением регистра символов), то пароль уровня 0 или 1 удаляется.
- Если указанный пароль содержит более 14 символов, пароль iSeries NetServer для пользовательского профайла удаляется.
- Системные значения паролей применяются только к новым паролям уровня 2 и не применяются к создаваемым системой паролям уровня 0 и 1 и паролям iSeries NetServer (если они создаются).

Изменение значения QPWDLVL с 2 на 3

Если на уровне QPWDLVL 2 система работает достаточно стабильно, администратор может принять решение о переходе на уровень QPWDLVL 3 для повышения надежности защиты паролей.

На уровне 3 удаляются все пароли iSeries NetServer, поэтому перед настройкой уровня 3 необходимо убедиться, что пароли iSeries NetServer больше не нужны.

На уровне QPWDLVL 3 все пароли уровней 0 и 1 удаляются. С помощью команд DSPAUTUSR и PRTUSRPRF администратор может найти профайлы, в которых нет паролей уровня 2 или 3.

Настройка более низкого уровня паролей

Даже если обратный переход к более низкому системному значению QPWDLVL возможен, он может вызвать некоторые затруднения. Вообще говоря, чаще всего обратный переход к более низкому системному значению QPWDLVL невозможен. Тем не менее, в некоторых случаях вы можете присвоить QPWDLVL более низкое значение.

В приведенных ниже разделах описаны действия по обратному переходу к более низкому уровню паролей.

Изменение значения QPWDLVL с 3 на 2: Выполнить такой переход относительно несложно. Если системное значение QPWDLVL равно 2, то администратор должен определить, требуется ли какому-либо пользовательскому профайлу пароль iSeries NetServer или пароль уровня 1 или 0, и если да, то изменить пароль в профайле на допустимое значение.

Кроме того, может потребоваться изменить системные значения паролей на значения, допускающие применение паролей iSeries NetServer и паролей уровня 0 или 1, если такие пароли нужны.

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, администратор должен найти все профайлы, в которых нет паролей уровня 0 или 1, с помощью команд DSPAUTUSR или PRTUSRPRF TYPE(*PWDINFO). Если после изменения значения QPWDLVL для работы с пользовательским профайлом будет необходим пароль, администратор должен создать пароль уровня 0 или 1 одним из следующих способов:

- Изменить пароль пользовательского профайла с помощью команды CL CHGUSRPRF или CHGPWD или API QSYCHGPW. При этом в системе будет изменен пароль уровня 2 или 3; системой будет также создан эквивалентный пароль уровня 1 в верхнем регистре. Система сможет создать пароль уровня 1 только в случае выполнения всех следующих условий:
  - Длина пароля не превышает 10 символов.
  - Все символы пароля можно преобразовать в символы EBCDIC верхнего регистра A-Z, 0-9, @, #, $ и _ .
  - Первый символ пароля отличен от цифры и знака подчеркивания.

  Например, при изменении пароля на RainyDay система создаст пароль RAINYDAY уровня 0 или 1. Но при изменении пароля на Rainy Days In April система удалит пароль уровня 0 или 1 (поскольку длина пароля слишком велика и он содержит пробелы).

  Если не удается создать пароль уровня 0 или 1, система не отправляет об этом никаких сообщений.
- Войти в систему с помощью алгоритма, при котором пароль не шифруется (не применяется подстановка паролей). Если пароль введен верно и в профайле нет пароля уровня 0 или 1, то системой будет создан эквивалентный пароль уровня 1 в верхнем регистре. Система сможет создать пароль уровня 1 только в том случае, если выполнены все указанные выше условия.

После этого значение QPWDLVL можно изменить на 1. Когда новое значение вступит в силу (при следующей IPL), все пароли iSeries NetServer будут удалены из системы.

Изменение значения QPWDLVL с 2 на 0: Процедура изменения значения QPWDLVL с 2 на 1 аналогична предыдущей за исключением того, что все пароли iSeries NetServer будут сохранены в системе.

Изменение значения QPWDLVL с 1 на 0: После изменения значения QPWDLVL на 0 необходимо найти в системе те пользовательские профайлы, в которых не задан пароль iSeries NetServer. Это можно сделать с помощью команды DSPAUTUSR или PRTUSRPRF. Если пользовательскому профайлу необходим пароль iSeries NetServer, его можно создать, изменив пароль пользователя или войдя в систему с помощью алгоритма, не применяющего шифрование паролей.

После этого администратор может присвоить QPWDLVL значение 0.

Изменение стандартных паролей

Измените стандартные пароли, для того чтобы с их помощью нельзя было войти в систему iSeries.

__ Шаг 1. Убедитесь, во всех пользовательских профайлах пароли по умолчанию (совпадающие с именем профайла) были изменены. Для этого вы можете воспользоваться командой Анализировать пароли по умолчанию (ANZDFTPWD). (См. “Изменение паролей по умолчанию” на стр. 26.)

__ Шаг 2. Попытайтесь войти в систему с использованием пользовательских профайлов и паролей, перечисленных в Табл. 2. Эти пароли опубликованы, и именно их будут пробовать применить для входа в вашу систему в первую очередь. Если войти в систему с такими паролями удалось, вызовите команду Изменить пользовательский профайл (CHGUSRPRF) и измените пароль в соответствии с приведенными рекомендациями.

__ Шаг 3. Запустите Специальные сервисные средства и попробуйте войти в систему с помощью паролей, указанных в разделе Табл. 2. За дополнительной информацией обратитесь к разделу iSeries Information Center—>Защита—>Сервисные средства. Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

__ Шаг 4. Если вам удалось войти в DST с помощью одного из этих паролей, измените их. Инструкции по изменению ИД и паролей пользователей сервисных средств приведены в разделе iSeries Information Center—>Защита—>Сервисные средства. Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

__ Шаг 5. Убедитесь, что в систему нельзя войти, нажав клавишу Enter в меню входа в систему, не введя предварительно ИД пользователя и пароль. Проверьте это на нескольких меню. Если вам удалось войти в систему без ввода информации в меню Вход в систему, выполните одно из следующих действий:

- Измените уровень защиты на 40 или 50 (системное значение QSECURITY).

  Примечание: Это может повлиять на работу некоторых приложений.
- Измените все записи рабочих станций для интерактивных подсистем таким образом, чтобы они указывали на описания заданий, в которых указано USER(*RQD).

Таблица 2. Пароли для профайлов, поставляемых фирмой IBM

ИД пользователя	Пароль	Рекомендуемое значение
QSECOFR	QSECOFR[1]	Усложненное значение, известное только администратору системы. **Запишите заданный пароль и храните его в надежном месте.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Таблица 2. Пароли для профайлов, поставляемых фирмой IBM (продолжение)

ИД пользователя	Пароль	Рекомендуемое значение

Примечания:

1. По умолчанию значение *Ограничить срок действия пароля* для профайла QSECOFR равно *YES. При первом входе в установленную систему вы должны изменить пароль QSECOFR.
2. Эти профайлы необходимы для системных функций, но следует запретить их использование для входа в систему пользователей. При установке систем версии V3R1 и выше для этого пароля задано значение *NONE.

   При вызове команды CFGSYSSEC система задает для этих паролей значение *NONE.
3. Для запуска iSeries Access для Windows с применением TCP/IP в системе должен быть активен пользовательский профайл QUSER.

Таблица 3. Пароли специальных сервисных средств

Уровень DST	ИД пользователя[1]	Пароль	Рекомендуемое значение
Основные функции	11111111	11111111	Усложненное значение, известное только администратору системы[2]
Все функции	22222222	22222222[3]	Усложненное значение, известное только администратору системы[2]
Функции защиты	QSECOFR	QSECOFR[3]	Усложненное значение, известное только администратору системы[2]
Функция обслуживания	QSRV	QSRV[3]	Усложненное значение, известное только администратору системы[2]

Примечания:

1. ИД пользователя требуется только для операционной системы, предназначенной для PowerPC AS (RISC).
2. Если сотруднику сервисного представительство по аппаратному обеспечению потребуется войти в систему с каким-либо ИД и паролем, после окончания его работы в системе измените пароль.
3. Срок действия пользовательского профайла сервисных средств истекает после первого использования.

Примечание: Пароли DST можно изменить только с помощью проверенного устройства. Это относится также и ко всем парам совпадающих паролей и ИД пользователей. Дополнительная информация о таких устройствах приведена в инструкциях по настройке Консоли управления, приведенных в iSeries Information Center.

Настройка параметров входа в систему

В Табл. 4 на стр. 23 перечислены некоторые значения, которые вы можете задать для усложнения несанкционированного входа в систему. Команда CFGSYSSEC служит для присвоения этим системным значениям рекомендуемых установок. Более подробно об этих системных значениях рассказано в главе 3 книги *iSeries Security Reference*.

Таблица 4. Системные значения для входа в систему

Имя системного значения	Описание	Рекомендуемое значение
QAUTOCFG	Должна ли система автоматически настраивать новые устройства.	0 (Нет)
QAUTOVRT	Число описаний виртуальных устройств, автоматически создаваемых системой, в том случае, если нет доступных для использования устройств.	0
QDEVRCYACN	Действие, выполняемое системой при повторном подключении устройства после ошибки.[1]	*DSCMSG
QDSCJOBITV	Время ожидания до завершения отключенного задания.	120
QDSPSGNINF	Будет ли показана информация о предыдущих действиях пользователя при входе в систему.	1 (Да)
QINACTITV	Время ожидания до завершения неактивного интерактивного задания.	60
QINACTMSGQ	Действие, выполняемое системой по истечении тайм-аута QINACTITV.	*ENDJOB
QLMTDEVSSN	Будет ли система запрещать пользователю входить в систему одновременно с нескольких рабочих станций.	1 (Да)
QLMTSECOFR	Будет ли разрешено пользователям с правами *ALLOBJ или *SERVICE работать только с указанных рабочих станций.	1 (Да)[2]
QMAXSIGN	Максимальное число последовательных неудачных попыток входа в систему (с неверным именем пользовательского профайла или паролем)	3
QMAXSGNACN	Действие, выполняемое системой по достижении значения QMAXSIGN.	3 (Отключить и пользовательский профайл, и устройство).

Примечания:

1. Если для сеанса явно указано описание устройства, система может отключать и заново подключать сеансы TELNET.
2. Если вы укажете для этого системного значения 1 (Да), то вам придется в явном виде предоставить пользователям с правами *ALLOBJ или *SERVICE права доступа к устройствам. Проще всего это осуществить, предоставив пользовательскому профайлу QSECOFR права доступа *CHANGE к конкретным устройствам.

Изменение сообщений об ошибках при входе в систему

Посторонним лицам, пытающимся проникнуть в вашу систему, надо по возможности мешать узнать степень эффективности их действий. Когда они видят на экране Вход в систему сообщение об ошибке `Пароль неверен`, они предполагают, что хотя бы ИД пользователя-то подобран правильно. Вы можете сбить злоумышленника с толку с помощью команды Изменить текст сообщения (CHGMSGD), изменив с ее помощью текст двух сообщений об ошибках при входе в систему. В Табл. 5 на стр. 24 предложен рекомендуемый текст.

Таблица 5. Сообщения об ошибках при входе в систему

ИД сообщения	Стандартный текст	Рекомендуемый текст
CPF1107	CPF1107 – Для пользовательского профайла указан неверный пароль.	Для входа в систему задана неверная информация **Примечание:** Не включайте в текст сообщения его ИД.
CPF1120	CPF1120 – Пользователь XXXXX не существует.	Для входа в систему задана неверная информация **Примечание:** Не включайте в текст сообщения его ИД.

Планирование активации пользовательских профайлов

Можно настроить пользовательские профайлы таким образом, чтобы они были доступны для входа в систему только в конкретное время дня или по конкретным дням недели. Например, вы можете разрешить использование профайла специалиста по проверке защиты системы только в его рабочее время. Можно также делать пользовательские профайлы со специальными правами доступа *ALLOBJ (включая и профайл QSECOFR) недоступными в нерабочие часы.

Для настройки автоматической активации и деактивации пользовательских профайлов служит команда Изменить запись расписания активации (CHGACTSCDE). Для каждого пользовательского профайла, который вы хотите настроить, можно создать запись его расписания.

Например, если вы хотите, чтобы профайл QSECOFR был доступен только в промежутке от 7 утра до 10 вечера, введите в меню CHGACTSCDE следующее:

```
              Изменить запись расписания активации (CHGACTSCDE)

Введите варианты, нажмите Enter.

Пользовательский профайл . . . . > QSECOFR       Имя
Время включения. . . . . . . . . > '7:00'        Время, *NONE
Время выключения . . . . . . . . > '22:00'       Время, *NONE
Дни недели . . . . . . . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                                  > *TUE
                                  > *WED
                                  > *THU
               + доп. значения    > *FRI
```

Рисунок 2. Меню Запланировать активацию профайла – пример

Фактически, вы можете настроить профайл QSECOFR так, чтобы он был доступным в течение ограниченного числа часов каждый день. Для выполнения большинства системных функций вы можете пользоваться другим пользовательским профайлом класса *SECOFR. Таким образом, вы повысите защищенность профайла, имя которого широко известно, от несанкционированного применения.

Вы можете периодически запускать команду Показать записи журнала контроля (DSPAUDJRNE) для печати записей CP (Изменить профайл). С помощью этих записей вы можете проверять, что система активирует и деактивирует пользовательские профайлы в соответствии с заданным вами расписанием.

Вы можете проверять правильность соблюдения заданного расписания другим способом - с помощью команды Печатать пользовательский профайл (PRTUSRPRF). Если вы укажете для типа отчета значение *PWDINFO, то в отчет будет включена информация о состоянии каждого выбранного пользовательского профайла. Например, если вы регулярно отключаете все пользовательские профайлы со специальными правами доступа *ALLOBJ, то сразу после их отключения вы можете запланировать запуск следующей команды:

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

Удаление неактивных пользовательских профайлов

В системе должны храниться только профайлы, необходимые для работы. Если какой-то пользовательский профайл стал не нужен вследствие того, что пользователь ушел из организации, удалите этот профайл. Если же сотрудник ушел из организации временно, но на длительный срок, то отключите (деактивируйте) его профайл. Лишние профайлы могут послужить средством для несанкционированного проникновения в вашу систему.

Автоматическое отключение пользовательских профайлов

С помощью команды Анализировать деятельность профайлов (ANZPRFACT) вы можете регулярно отключать пользовательские профайлы, которые находятся в состоянии неактивности в течение указанного числа дней. Вы должны задать для команды ANZPRFACT число дней неактивности, которое будет отслеживаться системой. Система будет собирать информацию о дате последнего использования профайла, а также о дате его восстановления и создания.

Система запланирует еженедельный запуск задания в 01:00, начиная с того дня, как вы зададите значение для команды ANZPRFACT. Задание проверяет все профайлы и отключает неактивные профайлы. Повторный вызов команды ANZPRFACT потребуется только для того, чтобы изменить число дней неактивности.

С помощью команды Изменить список активных профайлов (CHGACTPRFL) вы можете исключить некоторые профайлы из списка обрабатываемых командой ANZPRFACT. Команда CHGACTPRFL создает список пользовательских профайлов, которые не будут отключены командой ANZPRFACT не зависимо от того, как долго они длится их состояние неактивности.

При вызове системой команды ANZPRFACT в журнал контроля заносится запись CP для каждого отключенного пользовательского профайла. С помощью команды DSPAUDJRNE вы можете просмотреть список пользовательских профайлов, отключенных недавно.

Примечание: Система добавляет записи контроля только в том случае, если для значения QAUDCTL задано *AUDLVL, а для системного значения QAUDLVL задано *SECURITY.

Вы можете проверять правильность соблюдения заданного расписания другим способом - с помощью команды Печатать пользовательский профайл (PRTUSRPRF). Если вы укажете для типа отчета значение *PWDINFO, то в отчет будет включена информация о состоянии каждого выбранного пользовательского профайла.

Автоматическое удаление пользовательских профайлов

С помощью команды Изменить запись расписания истечения срока (CHGEXPSCDE) вы можете управлять удалением или отключением пользовательских профайлов.

Если известно, что пользователь не будет работать с профайлом в течение длительного времени, в можете запланировать удаление или отключение его пользовательского профайла.

При первом вызове команды CHGEXPSCDE она создаст запись расписания задания, которая будет запускаться каждые сутки в 00:01. Задание проверяет файл QASECEXP и определяет, подлежат ли какие-либо пользовательские профайлы удалению в этот день.

С помощью команды CHGEXPSCDE вы можете отключить или удалить пользовательский профайл. Если вы решите его удалить, то потребуется указать, что произойдет с объектами, принадлежащими этому пользователю. Перед тем как запланировать удаление профайла, следует изучить эти объекты. Например, если пользователь является владельцем программ, принимающих права доступа, то вы должны определить, примут ли эти программы нового владельца. Или не окажется ли у нового владельца больше прав доступа, чем необходимо (например, специальные права доступа). Возможно, потребуется создать новый пользовательский профайл с конкретными правами доступа, который будет являться владельцем программ, принимающих права доступа.

Еще следует проверить, не возникнут ли при удалении пользовательского профайла ошибки в каких-либо приложениях. Например, не указан ли в каких-либо описаниях заданий этот пользовательский профайл в качестве профайла по умолчанию?

С помощью команды Показать расписание истечения срока (DSPEXPSCD) вы можете просмотреть список профайлов, для которых запланировано отключение или удаление.

С помощью команды Показать пользователей с правами доступа (DSPAUTUSR) вы можете просмотреть список всех пользовательских профайлов вашей системы. Для удаления устаревших профайлов служит команда Удалить пользовательский профайл (DLTUSRPRF).

Примечание:: Отключение профайла осуществляется путем присвоения ему состояния *DISABLED. Отключенные профайлы не доступны для интерактивной работы. Вы не можете войти в систему с этим профайлом или назначить ему задание. Применение отключенного пользовательского профайла в пакетном задании возможно.

Изменение паролей по умолчанию

При создании нового пользовательского профайла ему по умолчанию присваивается пароль, совпадающий с именем профайла. Таким образом, если кому-то известны правила присвоения имен профайлам в вашей системе, а также тот факт, что в организации появился новый сотрудник, то у этого человека есть возможность проникнуть в систему.

При создании новых пользовательских профайлов обязательно измените пароль по умолчанию на уникальное, сложное значение. Сообщите новому пользователю его пароль конфиденциально, например, в письме “Добро пожаловать в систему”, в котором перечислены принятые стратегии защиты. Укажите для профайла этого пользователя значение PWDEXP(*YES) для того, чтобы ему пришлось изменить пароль после первого входа в систему.

Вы можете обнаружить наличие в каком-либо профайле пароля по умолчанию с помощью команды Анализировать пароли по умолчанию (ANZDFTPWD). При

печати отчета вам доступна опция выбора действия системы при обнаружении пароля, совпадающего с именем профайла (например, отключение профайла). Команда ANZDFTPWD печатает список таких профайлов и действия, предпринимаемые системой.

Примечание: К паролям, хранящиеся в вашей системе, применено одностороннее шифрование. Расшифровать их нельзя. Система зашифровывает введенный пароль и сравнивает его с хранящимся в системе точно так же, как она проверяет пароль при входе в систему. Если вы ведете контроль ошибок прав доступа (*AUTFAIL), то система добавит запись PW в журнал контроля для каждого пользовательского профайла, в котором применяется *не* пароль по умолчанию (в системах выпуска V4R1 и более ранних). Начиная с версии V4R2 при вызове команды ANZDFTPWD система не добавляет записи PW в журнал контроля.

Отслеживание неудачных попыток входа в систему

Если вы хотите предотвратить попытки несанкционированного доступа в вашу системе, вы можете воспользоваться командой PRTUSRPRF для отслеживания событий входа в систему и обработки пароля.

Вы можете использовать этот отчет следующим образом:

- Определите, не задан ли для каких-либо пользовательских профайлов срок действия пароля, превышающий системное значение, а если задан, то намерено ли. Например, в данном отчете у пользователя USERY срок действия пароля - 120 дней.
- Запускайте эту команду регулярно для отслеживания неудачных попыток входа в систему. Злоумышленник, который пытается взломать вашу систему, может знать, что ваша система выполняет какое-то действие после определенного числа неудачных попыток входа в систему. Поэтому он может каждую ночь выполнять меньшее число попыток, чем указано в значении QMAXSIGN, и вы не получите предупреждения. Но если вы будете каждое утро просматривать этот отчет, то заметите, что вход в систему с некоторыми профайлами часто заканчивается неудачно, и это вызовет ваши оправданные подозрения.
- С помощью этого отчета вы можете выявить пользовательские профайлы, которые давно не применялись, или пароли для которых не изменялись в течение долгого времени.

Хранение паролей

Согласно требованиям, предъявляемым некоторыми функциями работы в сети, на сервере iSeries предусмотрена защита паролей, которые могут быть расшифрованы. Такие пароли применяются, например, при установлении соединений SLIP. (См. раздел “Защита исходящих соединений” на стр. 132.)

На сервере iSeries такие пароли хранятся в защищенной области памяти, недоступной через интерфейсы пользователя. Доступ к этой области могут получать только специальные системные функции.

Например, пароль для исходящего соединения SLIP задается командой создания профайла конфигурации (WRKTCPPTP). Для работы с этой командой необходимы специальные права доступа *IOSYSCFG. Специально созданный сценарий соединения расшифровывает пароль и передает его процедуре вызова удаленной системы. Расшифрованный пароль не выводится на экран и не сохраняется в протоколе задания.

Администратор защиты должен определить, разрешается ли хранить в системе пароли, которые могут быть расшифрованы. Для этого в системе предусмотрено системное значение Сохранить идентификационные данные на сервере (QRETSVRSEC). По умолчанию оно равно 0 (Нет). Это означает, что в системе не сохраняются пароли, которые могут быть расшифрованы.

Если в вашей системе требуется хранить пароли, вы должны разработать специальные правила работы с ними. Например, если вы устанавливаете соединение с другой системой iSeries по протоколу SLIP, то в обеих системах должны быть созданы специальные пользовательские профайлы с ограниченными правами доступа. Тогда рассекречивание пароля удаленной системой не приведет к нарушению защиты локальной системы.

Глава 4. Настройка системы iSeries для применения средств защиты

В этом разделе приведены инструкции по настройке системы для работы со средствами защиты, входящими в состав OS/400. После установки OS/400 средства защиты уже готовы к применению. В следующих разделах описаны процедуры, которые вы можете выполнять с их помощью.

Защита средств защиты

После установки OS/400, объекты, связанные со средствами защиты, защищены. Для обеспечения их дальнейшей защиты не изменяйте настройки прав доступа к этим объектам.

Ниже приведено описание параметров защиты и требования к объектам средств защиты:

- Программы и команды средств защиты хранятся в библиотеке продуктов QSYS. Эти программы и команды поставляются с общими правами доступа *EXCLUDE. Многие команды средств защиты создают файлы в библиотеке QUSRSYS. При создании этим файлам присваиваются общие права доступа *EXCLUDE.

  Имена файлов, содержащих информацию для создания отчетов об изменениях, начинаются с QSEC. Имена файлов, содержащих информацию для управления пользовательскими профайлами, начинаются с QASEC. В этих файлах хранится конфиденциальная информация о вашей системе, поэтому не следует изменять общие права доступа к ним.
- Для направления печатаемого вывода средства защиты применяют стандартные настройки системы. В этих отчетах содержится конфиденциальная информация о вашей системе. Для направления этого вывода в защищенную очередь вывода, внесите соответствующие изменения в профайлы или описания задания для тех пользователей, которые будут работать со средствами защиты.
- Так как команды средств защиты отвечают за безопасность системы и так как они обращаются ко многим объектам системы, для них требуются специальные права доступа *ALLOBJ. Для некоторых команд требуются также специальные права доступа *SECADM, *AUDIT или *IOSYSCFG. Если вы хотите проверить успешность выполнения команд, войдите в систему с профайлом системного администратора. При этом вам не придется предоставлять частные права доступа командам средств защиты.

Предотвращение конфликтов файлов

Многие команды вывода отчета средств защиты создают файлы в базе данных, с помощью которого вы можете напечатать вариант отчета об изменениях. В разделе “Команды защиты и их меню” на стр. 30 перечислены имена файлов для всех команд. В каждый момент времени команда может быть запущена только из одного задания. В большинстве команд выполнение этого условия контролируется. Если вы вызовете команду в то время, пока она выполняется в другом задании, появится сообщение об ошибке.

Многие задания печати выполняются длительное время. При обработке отчетов в пакетном режиме или при добавлении их в планировщик заданий нужно внимательно следить, чтобы не возникло конфликтов файлов. Допустим, вам потребовалось

напечатать два варианта отчета PRTUSRPRF с разными критериями выбора. Если вы будете выполнять печать этих отчетов в пакетном режиме, то необходимо использовать очередь заданий, которая в каждый момент времени запускает только одно задание, что гарантирует последовательное выполнение заданий печати отчетов.

Если вы применяете планировщик заданий, то выполнение этих двух заданий нужно запланировать с большим промежутком времени между ними, чтобы печать первого варианта отчета закончилась до того, как начнется печать второго варианта.

Сохранение средств защиты

Вы можете сохранять программы средств защиты с помощью команды Сохранить систему (SAVSYS) или опции из меню Сохранить, запускающую эту команду.

Файлы средств защиты хранятся в библиотеке QUSRSYS. Рекомендуется сохранять эту библиотеку при выполнении обычных процедур работы в системе. Библиотека QUSRSYS содержит данные, предназначенные для многих лицензионных программ вашей системы. Дополнительная информация о командах и опциях сохранения библиотеки QUSRSYS приведена в Information Center.

Команды защиты и их меню

В этом разделе описаны команды и меню для средств защиты. Примеры применения этих команд приведены в различных разделах данного документа.

При работе со средствами защиты можно применять два меню:

- Меню SECTOOLS (Средства 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 средств защиты

В Табл. 6 приведено описание этих опций меню и связанных с ними команд:

Таблица 6. Команды работы с пользовательскими профайлами

Опция меню[1]	Команда	Описание	Файл базы данных
1	ANZDFTPWD	С помощью команды Анализировать пароли по умолчанию вы можете определить пользовательские профайлы, для которых пароль совпадает с их именем, и выполнить действие над такими профайлами.	QASECPWD[2]
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]

Таблица 6. Команды работы с пользовательскими профайлами (продолжение)

Опция меню[1]	**Команда**	**Описание**	**Файл базы данных**
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, постоянно активны (вплоть до тех пор, 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 деятельность 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 вы можете задать исключение для некоторых пользовательских профайлов.	QASECIDL[2]
5	DSPACTSCD	С помощью команды Показать расписание активации профайлов вы можете просмотреть или напечатать информацию расписания активации и отключения конкретных пользовательских профайлов. Это расписание задается командой CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	С помощью команды Изменить запись расписания активации вы можете настроить пользовательский профайл таким образом, что он будет доступен только в конкретные часы дня и в конкретные дни недели. Для каждого профайла, включенного в расписание, система создает записи расписания заданий с указанием времени его включения и отключения.	QASECACT[2]
7	DSPEXPSCD	С помощью команды Показать расписание истечения срока вы можете просмотреть или напечатать список пользовательских профайлов, для которых запланировано отключение или удаления из системы. Срок действия профайлов задается командой CHGEXPSCDE.	QASECEXP[2]

Таблица 6. Команды работы с пользовательскими профайлами (продолжение)

Опция меню[1]	Команда	Описание	Файл базы данных
8	CHGEXPSCDE	С помощью команды Изменить запись расписания истечения срока вы можете запланировать удаление пользовательского профайла. Вы можете временно отключить профайл или удалить его из системы окончательно. 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. Вы можете просмотреть список пользовательских профайлов, истечение срока которых запланировано, с помощью команды DSPEXPSCD.	QASECEXP[2]
9	PRTPRFINT	С помощью команды Печатать содержимое профайла вы можете напечатать отчет с указанием числа записей пользовательского профайла. Число записей определяет размер пользовательского профайла.	

Примечания:

1. Это опции меню SECTOOLS.
2. Этот файл находится в библиотеке QUSRSYS.

Для просмотра дополнительных опций меню нажмите клавишу Page down. В Табл. 7 описаны опции меню и связанные с ними команды, служащие для контроля за действиями:

Таблица 7. Команды контроля за действиями

Опция меню[1]	Команда	Описание	Файл базы данных
10	CHGSECAUD	Команда Изменить параметры контроля за действиями служит для настройки контроля за действиями и для изменения соответствующих системных значений. Если в момент запуска команды CHGSECAUD журнал контроля за действиями (QAUDJRN) в системе не существует, то он автоматически создается. У команды CHGSECAUD есть несколько опций, упрощающих задание системного значения QAUDLVL (уровень контроля). Вы можете указать значение *ALL для активации всех возможных параметров уровней контроля или значение *DFTSET для активации наиболее часто используемых параметров (*AUTFAIL, *CREATE, *DELETE, *SECURITY и *SAVRST). **Примечание:** Если вы применяете средства защиты для настройки контроля за действиями, то рекомендуется запланировать управление получателями журнала контроля. В противном случае быстро возникнет проблема нехватки дискового пространства.	

Таблица 7. Команды контроля за действиями (продолжение)

Опция меню[1]	Команда	Описание	Файл базы данных
11	DSPSECAUD	Команда Показать параметры контроля за действиями служит для просмотра информации о журнале контроля за действиями и о соответствующих системных значениях.	

Примечания:

1. Это опции меню SECTOOLS.

Применение меню SECBATCH

Ниже приведена первая часть меню SECBATCH:

```
SECBATCH         Запустить или запланировать обработку отчетов о защите 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 файлу
    12. Частные права доступа к файлу
    13. Права доступа к папке
```

При выборе опции этого меню появляется меню Передать задание на выполнение (SBMJOB). Если вы хотите изменить опции по умолчанию для команды, нажмите F4 (Приглашение) в строке *Вызываемая команда*.

Для просмотра Расписания обработки отчетов в пакетном режиме нажмите клавишу Page down в меню SECBATCH. С помощью опций этой части меню вы можете, например, настроить регулярный запуск отчетов об изменениях в вашей системе. Для перехода к дополнительным опциям меню нажмите клавишу Page down. При выборе опции в этом разделе меню появляется меню Добавить запись расписания заданий (ADDJOBSCDE).

Для выбора других значений для отчета, 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 Передать отчеты на обработку в пакетном режиме

В разделе Табл. 8 на стр. 34 описаны опции меню и связанные с ними команды, служащие для обработки отчетов о защите.

При вызове команд вывода запросов о защите система печатает только ту информацию, которая отвечает одновременно указанным критериям выбора и критериям выбора для данной функции. Например, описания задания, в которых указано имя пользовательского профайла, требуют защиты. Поэтому 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 для параметра USER указан пользовательский профайл.

Аналогично, при запросе 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 каком-либо отчете при печати было включено меньше информации, чем вы ожидали, обратитесь к электронной справке и определите критерии выбора для этого отчета.

Таблица 8. Команды обработки отчетов о защите

Опция меню[1]	**Команда**	**Описание**	**Файл базы данных**
1, 40	PRTADPOBJ	С помощью команды Печатать принимающие объекты вы можете напечатать список объектов, принимающие права доступа указанного пользовательского профайла. Вы можете указать отдельный профайл, шаблон имени профайла (например, все имена, начинающиеся на Q) или все профайлы системы. Возможны два варианта вывода этого отчета. Полный отчет включает список всех принимающих объектов, отвечающих критериям 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	Команда Показать записи журнала контроля служит для просмотра или печати информации о записях журнала контроля за действиями. Вы можете выбрать группу записей по типу, по пользователям или по периоду времени.	QASYxxJ4[3]
3, 42	PRTPVTAUT *AUTL	Команда Печатать частные права доступа для объектов *AUTL выводит все списки прав доступа системы. Для каждого списка в отчете указаны пользователи, у которых есть права доступа к нему, и сами права доступа. Эта информация полезна при анализе источников прав доступа к объектам вашей системы. Возможны три варианта вывода этого отчета. Полный отчет включает все списки прав доступа системы. В отчете об изменениях перечислены все изменения и добавления с момента предыдущей обработки этого отчета. В отчете об удалениях перечислены пользователи, чьи права доступа к спискам прав доступа были удалены с момента предыдущей обработки этого отчета. При печати полного отчета вы можете выбрать печать списка объектов, защищенных списком прав доступа. Для каждого списка прав доступа система создаст отдельный отчет.	QSECATLOLD[2]

Таблица 8. Команды обработки отчетов о защите (продолжение)

Опция меню[1]	**Команда**	**Описание**	**Файл базы данных**
6, 45	PRTCMNSEC	Команда Печатать параметры защиты связи служит для печати параметров защиты объектов системы, связанных со средствами связи. Эти параметры определяют возможности доступа пользователей и заданий к вашей системе. Эта команда создает два отчета: в первом перечислены настройки списков конфигураций системы, а второй - параметры защиты для описаний линий связи, контроллеров и описаний устройств. Каждый отчет может быть выведен в полном виде и в виде списка изменений.	QSECCMNOLD[2]
15, 54	PRTJOBDAUT	Команда Печатать 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 указаны также специальные права доступа для заданного пользовательского профайла. Возможны два варианта вывода этого отчета. Полный отчет включает список всех объектов описаний заданий, отвечающих критериям выбора. В отчете об изменениях перечислены различия между объектами описаний заданий, находящимися в системе в настоящий момент, и объектами, которые находились в системе в момент предыдущей обработки этого отчета.	QSECJBDOLD[2]
См. примечание 4	PRTPUBAUT	С помощью команды Печатать общедоступные объекты вы можете напечатать список объектов, общие права доступа к которым отличны от *EXCLUDE. При вызове команды требуется указать тип объекта и одну или несколько библиотек для отчета. Команда PRTPUBAUT служит для печати информации об объектах, доступ к которым есть у всех пользователей системы. 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.	QPBxxxxxx[5]

Таблица 8. Команды обработки отчетов о защите (продолжение)

Опция меню[1]	**Команда**	**Описание**	**Файл базы данных**
См. примечание 5.	PRTPVTAUT	Команда Печатать частные права доступа служит для вывода списка частных прав доступа к объектам указанного типа в указанной библиотеке. С помощью этого отчета вы можете определить источники прав доступа к объектам. 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 с момента предыдущей обработки этого отчета.	QPVxxxxxx[5]
24, 63	PRTQAUT	С помощью команды Печатать отчет об очереди вы можете напечатать настройки защиты для очередей ввода и очередей заданий в вашей системе. Эти параметры определяют пользователей, которые могут просматривать и изменять записи в этих очередях. 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 объектами очередей вывода и очередей заданий, находящимися в системе в настоящий момент, и объектами, которые находились в системе в момент предыдущей обработки этого отчета.	QSECQOLD[2]
25, 64	PRTSBSDAUT	С помощью команды Печатать описание подсистемы вы можете напечатать записи параметров связи, влияющих на защиту, для описаний подсистем вашей системы. 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. Возможны два варианта вывода этого отчета. Полный отчет включает список всех описаний подсистем, отвечающих критериям выбора. В отчете об изменениях перечислены различия между объектами описаний подсистем, находящимися в системе в настоящий момент, и объектами, которые находились в системе в момент предыдущей обработки этого отчета.	QSECSBDOLD[2]

Таблица 8. Команды обработки отчетов о защите (продолжение)

Опция меню[1]	Команда	Описание	Файл базы данных
26, 65	PRTSYSSECA	Команда Печатать системные атрибуты защиты служит для печати списка системных значений и сетевых атрибутов, влияющих на защиту. В отчете указано текущее значение и рекомендуемое значение.	
27, 66	PRTTRGPGM	С помощью команды Печатать программы триггера вы можете напечатать список программ триггера, связанных с файлами базы данных вашей системы. Возможны два варианта вывода этого отчета. В полном отчете перечислены все назначенные программы триггера, отвечающие критериям выбора. В отчете об изменениях перечислены программы триггера, которые были назначены с момента последней обработки этого отчета.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	Команда Печать пользовательских объектов позволяет напечатать список пользовательских объектов (объектов, не поставляемых фирмой IBM), расположенных в библиотеке. Этот отчет может пригодиться для печати списка пользовательских объектов какой-либо библиотеки (например, QSYS) из списка системных библиотек. 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.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Команда Печатать пользовательский профайл 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, пароле или уровне пароля.	
30, 69	PRTPRFINT	С помощью команды Печатать содержимое профайла вы можете напечатать отчет с указанием числа записей пользовательского профайла.	
31, 70	CHKOBJITG	С помощью команды Проверить целостность объекта вы можете определить, были ли рабочие объекты (например, программы) изменены без использования компилятора. Эта команда позволяет выявить попытки внедрения в вашу систему вируса или несанкционированного изменения действия программы. Подробная информация о команде CHKOBJITG приведена в книге *iSeries Security Reference*.	

Таблица 8. Команды обработки отчетов о защите (продолжение)

Опция меню[1]	Команда	Описание	Файл базы данных
Примечания: 1. Это опции меню SECBATCH. 2. Этот файл находится в библиотеке QUSRSYS. 3. xx - это тип записи журнала, длиной в два символа. Например, файл вывода для записей журнала типа AE будет выглядеть как QSYS/QASYAEJ4. Модели файлов вывода описаны в Приложении F книги *iSeries Security Reference*. 4. Меню SECBATCH включает опции для типов объектов, с которыми обычно работают администраторы защиты. Например, опция 11 или 50 для запуска команды PRTPUBAUT для объектов *FILE. Вы можете указать тип объекта с помощью общих опций (18 и 57). 5. Меню SECBATCH включает опции для типов объектов, с которыми обычно работают администраторы защиты. Например, опция 12 или 51 для запуска команды PRTPVTAUT для объектов *FILE. Вы можете указать тип объекта с помощью общих опций (19 и 58). 6. Символы xxxxxx в имени файла обозначают тип объекта. Например, файл для программных объектов называется QPBPGM для общих прав доступа и QPVPGM - для частных прав доступа. Этот файл хранится в библиотеке QUSRSYS. Он содержит элемент для каждой библиотеки, для которой вы создавали отчет. Имя элемента совпадает с именем библиотеки.			

Команды настройки параметров защиты

В Табл. 9 описаны команды, предназначенные для настройки защиты вашей системы. Эти команды вызываются из меню SECTOOLS.

Таблица 9. Команды настройки системы

Опция меню[1]	Команда	Описание	Файл базы данных
60	CFGSYSSEC	Команда Настроить защиту системы служит для задания рекомендуемых установок для системных значений, влияющих на защиту. Эта команда задает также параметры контроля за действиями в вашей системе. Действие команды описано в разделе “Значения, устанавливаемые командой Настроить защиту системы” на стр. 39. **Примечание:** Для получения рекомендаций по настройке защиты в конкретной системе запустите вместо этой команды Мастер настройки защиты iSeries или Советник по настройке защиты iSeries. Информация по этим программам приведена в разделе Глава 2, “Мастер настройки защиты и планировщик конфигурации защиты iSeries”, на стр. 11.	
61	RVKPUBAUT	С помощью команды Аннулировать общие права доступа вы можете задать для набора команд, требующих защиты, общие права доступа *EXCLUDE. Действие этого команды описано в разделе “Функции команды Аннулировать общие права доступа” на стр. 41.	
Примечания: 1. Это опции меню SECTOOLS.			

Значения, устанавливаемые командой Настроить защиту системы

В Табл. 10 перечислены системные значения, устанавливаемые при выполнении команды CFGSYSSEC. Команда CFGSYSSEC запускает программу QSYS/QSECCFGS.

Таблица 10. Значения, устанавливаемые командой CFGSYSSEC

Имя системного значения	Устанавливается равным	Описание системного значения
QALWOBJRST	*NONE	Можно ли восстанавливать программы режима системы и программы, принимающие права доступа
QAUTOCFG	0 (Нет)	Автоматическая настройка новых устройств
QAUTOVRT	0	Число описаний виртуальных устройств, создаваемых системой при отсутствии доступных устройств.
QDEVRCYACN	*DSCMSG (Отправлять сообщение при отключении)	Действие системы при повторной установке соединения
QDSCJOBITV	120	Продолжительность ожидания системы перед выполнением действия над отключенным заданием
QDSPSGNINF	1 (Да)	Показывать ли пользователям меню входа в систему
QINACTITV	60	Продолжительность ожидания системы перед выполнением действия над неактивным 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)	Выключать ли рабочую станцию или пользовательский профайл при достижении максимального значения, указанного в QMAXSIGN.
QRMTSIGN	*FRCSIGNON	Способ управления запросами на вход в систему (удаленный вход или TELNET).
QRMTSVRATR	0 (Запретить)	Разрешает удаленный анализ неполадок в системе.
QSECURITY[1] на стр. 40	50	Устанавливаемый уровень защиты
QVFYOBJRST	3 (Проверять подписи при восстановлении)	Проверяет объект при восстановлении
QPWDEXPITV	60	Периодичность изменения паролей пользователей
QPWDMINLEN	6	Минимальная длина пароля
QPWDMAXLEN	8	Максимальная длина пароля
QPWDPOSDIF	1 (Да)	Должны ли различаться символы нового и старого пароля, стоящие в одних и тех же позициях
QPWDLMTCHR	См. примечание 2 на стр. 40	Символы, которые нельзя указывать в пароле
QPWDLMTAJC	1 (Да)	Запрещать ли использование в паролях цифр в соседних позициях
QPWDLMTREP	2 (Запретить использование одинаковых символов в соседних позициях)	Запрещать ли использование в пароле одинаковых символов

Таблица 10. Значения, устанавливаемые командой CFGSYSSEC (продолжение)

Имя системного значения	Устанавливается равным	Описание системного значения
QPWDRQDDGT	1 (Да)	Должен ли пароль 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.
QPWDVLDPGM	*NONE	Пользовательская программа выхода, вызываемая системой для проверки паролей

Примечания:

1. Если текущее значение QSECURITY меньше либо равно 40, то прежде чем устанавливать более высокий уровень защиты, прочтите главу 2 книги *iSeries Security Reference*.
2. Набор запрещенных символов указан в сообщении с идентификатором CPXB302 в файле сообщений QSYS/QCPFMSG в виде AEIOU@$#. Для изменения набора запрещенных символов вызовите команду CHGMSGD (Изменить описание сообщения). Системное значение QPWDLMTCHR не применяется для уровня паролей 2 и 3.

Кроме того, команда CFGSYSSEC устанавливает пустой пароль (*NONE) для следующих пользовательских профайлов, поставляемых фирмой IBM:

QSYSOPR
QPGMR
QUSER
QSRV
QSRVBAS

И, наконец, команда CFGSYSSEC включает режим управления защитой с помощью команды CHGSECAUD (Изменить контроль за действиями). Команда CFGSYSSEC включает режим контроля за действиями пользователей и контроль объектов и, кроме того, задает в команде CHGSECAUD набор действий, которые должны контролироваться по умолчанию.

Создание программы

Если некоторые значения не подходят для вашей системы, вы можете создать свою собственную программу, запускаемую при вводе команды. Для этого:

__ Шаг 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*.

__ Шаг 2. Внесите в текст программы необходимые изменения. Откомпилируйте ее. Помните: для того чтобы при этом случайно *не удалить* стандартную программу IBM QSYS/QSECCFGS, у вашей программы должно быть другое имя.

__ Шаг 3. С помощью команды CHGCMD (Изменить команду) 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)
```

Примечание: После изменения программы QSYS/QSECCFGS фирма IBM не может гарантировать ее надежность и пригодность для

какой-либо цели. При этом подразумеваемые гарантии ее коммерческой ценности и пригодности для какой-либо цели аннулируются.

Функции команды Аннулировать общие права доступа

Команда Аннулировать общие права доступа (RVKPUBAUT) позволяет установить для набора команд или программ общие права доступа *EXCLUDE. Она запускает программу с именем QSYS/QSECRVKP. Стандартная программа QSECRVKP аннулирует общие права доступа (устанавливая значение *EXCLUDE) для команд и интерфейсов прикладных программ (API), перечисленных в таблицах Табл. 11 и Табл. 12, соответственно. В новой системе общие права доступа к командам и API равны *USE.

Команды и интерфейсы, перечисленные в таблицах Табл. 11 и Табл. 12, 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 для всех остальных пользователей.

При вызове команды RVKPUBAUT задается библиотека, в которой хранятся команды. По умолчанию применяется библиотека QSYS. Если в вашей системе несколько национальных языков, эту команду необходимо вызвать для всех библиотек QSYSxxx.

Таблица 11. 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. 12, находятся в библиотеке QSYS:

Таблица 12. Программы, общие права доступа к которым устанавливаются командой RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

При выполнении команды RVKPUBAUT для корневого каталога устанавливаются общие права доступа *USE (если еще не установлены права доступа *USE или ниже).

Создание программы

Если некоторые значения не подходят для вашей системы, вы можете создать свою собственную программу, запускаемую при вводе команды. Для этого выполните следующие действия:

__ Шаг 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*.

__ Шаг 2. Внесите в текст программы необходимые изменения. Откомпилируйте ее. Для того чтобы при этом случайно *не удалить* стандартную программу IBM QSYS/QSECRVKP, у вашей программы должно быть другое имя.

__ Шаг 3. С помощью команды CHGCMD (Изменить команду) 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)
```

Примечание: После изменения программы QSYS/QSECRVKP фирма IBM не может гарантировать ее надежность и пригодность для какой-либо цели. При этом подразумеваемые гарантии ее коммерческой ценности и пригодности для какой-либо цели аннулируются.

Часть 2. Дополнительные функции защиты iSeries

Глава 5. Защита информации и права доступа к объектам

Задача системного администратора заключается в обеспечении защиты информационных ресурсов вашей организации без помех для работы пользователей системы. Необходимо обеспечить пользователей правами, необходимыми для выполнения их заданий, но не достаточными для доступа к настройкам системы и для их изменения.

Совет по организации защиты

Не рекомендуется слишком сильно ограничивать права пользователей. Стремясь расширить свои возможности, пользователи могут начать обмениваться паролями.

В операционной системе OS/400 реализована интегрированная защита объектов. Для доступа к объектам пользователи должны использовать интерфейсы, предоставляемые системой. Например, если вы хотите обратиться к файлу базы данных, вы должны применить команду или программу, специально для этого предназначенную. Нельзя использовать команду, служащую для обращения к очереди сообщений или к протоколу задания.

Когда вы запрашиваете объект через системный интерфейс, система проверяет, есть ли у вас права доступа к данному объекту, требуемые для данного интерфейса. Права доступа к объекту - это мощное и гибкое средство защиты информационных ресурсов системы. Задача системного администратора заключается в том, чтобы задать схему эффективной защиты объектов и впоследствии управлять этой схемой и обслуживать ее.

Автоматическое назначение прав доступа к объектам

При обращении пользователя к объекту операционная система проверяет его права доступа. Но если уровень защиты системы (системное значение QSECURITY) равен 10 или 20, то пользователю автоматически присваиваются права на доступ к любому объекту, так как каждый профайл системы обладает специальными правами доступа *ALLOBJ.

Совет по настройке прав доступа к объектам: Если вы не знаете, применяется ли в системе защита объектов, просмотрите системное значение QSECURITY (уровень защиты). Если QSECURITY равно 10 или 20, то защита объектов не действует.

Необходимо запланировать и подготовиться к изменению уровня защиты на 30 или выше. В противном случае доступ к информации для пользователей может оказаться закрыт.

В разделе **Basic system security and planning** справочной системы Information Center приведены инструкции по анализу приложений и выбору защиты объектов. Если вы не применяете защиту объектов или если вы хотите заменить устаревшую или запутанную схему защиты, обратитесь к данному разделу для вспомогательной информацией.

Управление доступом через меню

Изначально сервер iSeries был разработан как модификация S/36 и S/38. Многие продукты iSeries ранее являлись продуктами S/36 или S/38. Для управления возможностями пользователей в этих ранних выпусках администраторы защиты часто применяли технологию, которая называется **защита через меню** или **управление доступом через меню**.

Эта технология подразумевает, что, войдя в систему, пользователь попадает в меню. Пользователь может выполнять только те функции, которые доступны из этого меню. Командная строка, из которой можно было бы выполнить другие функции, недоступна. Теоретически, администратору защиты не требуется задавать права доступа к объектам, так как возможности пользователя определяются меню и программами.

На сервере iSeries предусмотрено несколько параметров пользовательских профайлов, предназначенных для управления доступом через меню:

- Параметр **Начальное меню** (INLMNU) определяет меню, которое будет первым показано пользователю при входе в систему.
- Параметр **Начальная программа** (INLPGM) задает программу настройки, которая будет запущена до того, как пользователь увидит меню. С помощью параметра INLPGM можно также ограничить возможности пользователя, разрешить ему работать всего с одной программой.
- С помощью параметра **Ограничить возможности** (LMTCPB) можно задать ограниченный набор команд, с которыми пользователю будет разрешено работать. Этот параметр запрещает пользователю менять начальную программу или начальное меню в окне Вход в систему. (Параметр LMTCPB накладывает ограничения только на команды, вводимые в командной строке).

Ограничения на управление доступом через меню

За последние несколько лет компьютерные технологии шагнули далеко вперед. Появились новые средства, такие как программы обработки запросов и электронные таблицы, позволяющие пользователям самим выполнять некоторые задачи программирования, снимая таким образом часть нагрузки с отделов IS. Отдельные средства, такие как SQL или ODBC, предоставляют возможность просматривать и изменять информацию. Организовать работу с этими средствами через систему меню очень сложно.

Компьютеры (как автономные, так и объединенные в сети), быстро вытесняют рабочие станции (“зеленые экраны”) с ограниченными возможностями. Если ваша система подключена к сети, пользователи могут войти в нее, минуя меню входа в систему.

Если системный администратор намерен продолжать управлять доступом через меню, он столкнется с двумя проблемами:

- Если ему удастся ограничить возможности пользователей некоторым набором меню, они не смогут воспользоваться многими современными средствами работы.
- Если же он допустит какие-либо ошибки в настройке набора меню, то возникнет вероятность несанкционированного обращения к конфиденциальной информации, безопасность которой собственно и должен был гарантировать доступ через меню. Если ваша система подключена к сети, эффективность работы с доступом через меню значительно уменьшается. Например, параметр LMTCPB применим только к командам, вызываемым из командной строки в интерактивном режиме. Этот параметр не будет иметь никакого действия, если его применять в запросах сеансов связи, например, при передаче файлов PC, по FTP или в удаленных командах.

Дополнение возможностей системы меню средствами защиты объектов

Поскольку появилось много новых способов подключения к системам, эффективная схема защиты iSeries не должна включать в себя только средства управления доступом через меню. В данном разделе предложены пути перехода к среде с защитой объектов, дополняющей возможности системы меню.

В разделе *Basic system security and planning* справочной системы Information Center приведены инструкции по анализу прав доступа к объектам, необходимых пользователям для запуска текущих приложений. Следует разделить всех пользователей на группы и присвоить каждой группе соответствующие права доступа. Этот подход вполне логичен. Но если система используется уже много лет и в ней работает много приложений, задача анализа приложений и распределения прав доступа к объектам может оказаться весьма сложной.

Совет по настройке прав доступа к объектам: От управления доступом через меню рекомендуется перейти к применению меню в сочетании с программами, принимающими права доступа своих владельцев. Обязательно установите защиту для программ, принимающих права доступа, и для пользовательских профайлов, являющихся их владельцами.

Текущие меню могут применяться во временной рабочей среде, в то время как выполняется последовательный анализ приложений и объектов. Ниже приведен пример применения меню Запись заказа (OEMENU) в сочетании со связанными файлами и программами.

Пример: Настройка временной рабочей среды

Прежде всего перечислим в этом примере предполагаемые условия и требования:

- Все файлы хранятся в библиотеке ORDERLIB.
- Вы не знаете имен всех файлов. Вы также не знаете, какие права доступа к различным файлам нужны для опций меню.
- Это меню и все программы, вызываемые из него, находятся в библиотеке ORDERPGM.
- Вы хотите, чтобы все пользователи, входящие в систему, могли обращаться к информации всех файлов заказов, файлов заказчиков и файлов товаров (например, через запросы или через электронные таблицы).
- Изменять файлы могут только те пользователи, для которых текущим меню входа является OEMENU. Для этой операции они должны применять программы данного меню.
- В отличие от администраторов защиты у прочих пользователей системы специальных прав доступа *ALLOBJ или *SECADM нет.

Для того чтобы в среде управления доступом через меню появилась возможность обрабатывать запросы, выполните следующие действия:

__ Шаг 1. Составьте список пользователей, у которых начальным меню является OEMENU.

Для вывода списка сред для всех пользовательских профайлов системы воспользуйтесь командой Печатать пользовательский профайл (PRTUSRPRF *ENVINFO). В вывод будет включена информация о начальном меню, начальной программе и текущей библиотеке. На рис. 7 на стр. 64 приведен пример выводимого отчета.

__ Шаг 2. Убедитесь, что владельцем объекта OEMENU (он должен являться объектом типа *PGM или *MENU) является пользовательский профайл, не применяемый для входа в систему. Этот профайл должен быть отключен или в качестве значения его пароля должно быть задано *NONE. Для данного примера допустим, что владельцем программного объекта OEMENU является OEOWNER.

__ Шаг 3. Проверьте, что пользовательский профайл-владелец программного объекта OEMENU не является профайлом группы. Вы можете воспользоваться следующей командой:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ Шаг 4. Измените параметры программы OEMENU так, чтобы она принимала права доступа от пользовательского профайла OEOWNER. (С помощью команды CHGPGM задайте для параметра USRPRF значение *OWNER.)

Примечание: Объекты типа *MENU не могут принимать права доступа. Если OEMENU является объектом типа *MENU, вы можете данный пример изменить таким образом, чтобы в нем выполнялась одна из следующих операций:

- Создать программу для просмотра меню.
- Применять принятые права доступа для программ, запускаемые при выборе пользователем опций в меню OEMENU.

__ Шаг 5. Задайте общие права доступа *USE ко всем файлам библиотеки ORDERLIB с помощью следующих двух команд:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*USE)
```

Помните, что если вы выберете прав доступа *USE, пользователи смогут копировать файлы путем передачи файлов PC или по протоколу FTP.

__ Шаг 6. Присвойте профайлу-владельцу программ меню права доступа *ALL к файлам, введя следующую команду:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

Для большинства приложений прав доступа к файлам *CHANGE вполне достаточно. Но в некоторых приложениях может потребоваться выполнить функции (например, очистка элементов физических файлов), для которых потребуется больше прав доступа. Итак, вы можете можно проанализировать приложения системы и предоставить пользователям минимальные права доступа к ним. Но во временной рабочей среде могут произойти сбои в работе приложений, которые можно избежать, приняв права доступа *ALL.

__ Шаг 7. Ограничьте прав доступа к программам из библиотеки заказов с помощью команды:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
     AUT(*EXCLUDE)
```

__ Шаг 8. Предоставьте права доступа профайла OEOWNER программам в этой библиотеке с помощью команды:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
     AUT(*USE)
```

__ Шаг 9. Предоставьте пользователям из списка, составленного на этапе 1 права доступа к программам меню, введя следующую команду для каждого пользователя:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(имя_пользовательского_профайла) AUT(*USE)
```

После выполнения этих действий все пользователи системы, которые не были явно исключены, смогут обращаться (но не изменять) к файлам библиотеки ORDERLIB. Пользователи, у которых есть права доступа к программе OEMENU смогут применять программы, включенные в меню, для обновления файлов в библиотеке ORDERLIB. Эта операция разрешена только пользователям с правами доступа к программе OEMENU. Таким образом, файлы защищены комбинированием защиты объекта и управления доступом к меню.

Выполнив такие действия для всех библиотек, содержащих пользовательские данные, вы создадите простую схему управления обновлениями базы данных. Этот способ гарантирует, что обновление файлов базы данных выполняется пользователями только с помощью разрешенных меню и программ. В то же время база данных доступна для просмотра, анализа и копирования пользователям, работающим со средствами приятия решений или подключающимся по линиям связи из другой системы или с PC.

Совет по настройке прав доступа к объектам: Если система подключена к сети, права доступа *USE предоставляют пользователям довольно широкие возможности. Например, если у вас есть права доступа *USE к файлу, вы можете скопировать этот файл в другую систему (в том числе и на PC) по протоколу FTP.

Применение защиты библиотек совместно с ограничением доступа через меню

Для обращения к объекту в библиотеке у вас должны быть как права доступа к объекту, так и к библиотеке. Для большинства операций к библиотеке требуются права доступа *EXECUTE или *USE.

В зависимости от ситуации вы можете применять права доступа к библиотеке как простейшее средство защиты объектов. Например, предположим, что в примере с меню Записи заказов любой пользователь с правами доступа к этому меню может работать со всеми программами из библиотеки ORDERPGM. Вместо защиты отдельных программ вы можете задать общие права доступа *EXCLUDE к библиотеке ORDERPGM. После этого вы можете предоставить выбранным пользовательским профайлам права доступа *USE к этой библиотеке для того, чтобы эти пользователи могли работать с программами, хранящимися в ней. (Предполагается, что в качестве общих прав доступа к программам задано *USE или выше).

Задание прав доступа к библиотеке - это простой и эффективный способ администрирования доступа к объектам. Но необходимо четко знать содержимое этих библиотек, чтобы случайно не открыть доступ к другим объектам.

Настройка принадлежности объекта

Принадлежность объектов системы - это важный элемент схемы управления доступом к объектам. По умолчанию владельцу объекта присваиваются права доступа *ALL к его объекту. В Главе 5 книги *iSeries Security Reference* приведены рекомендации и примеры для планирования принадлежности объектов. Ниже вы можете найти несколько советов:

- В общем случае профайлы групп не должны являться владельцами объектов. В противном случае у всех элементов группы, кроме тех, которые исключены явно, будут права доступа *ALL к этому объекту.

- Если вы работаете с принятыми правами доступа, то определите, будут ли пользовательским профайлам-владельцам программ принадлежать также объекты приложений, например, файлы. В некоторых случаях нежелательно, чтобы пользователи, работающие с программами, принимающими права доступа, обладали правами доступа *ALL к файлам.

Если вы работаете с Навигатором iSeries, необходимые изменения можно внести с помощью функции **стратегий** защиты. Дополнительная информация приведена в iSeries Information Center (подробнее см. “Необходимая и полезная информация” на стр. xii).

Права доступа к объектам системных команд и программ

Ниже приведены предложения по ограничению прав доступа к объектам, поставляемым фирмой IBM:

- Если в системе установлено несколько национальных языков, то в ней существует несколько системных (QSYS) библиотек. Каждому национальному языку в системе соответствует библиотека QSYSxxxx. Если вы управляете доступом к системным командам с помощью прав доступа к объектам, то не забудьте настроить защиту команды как в библиотеке QSYS, так и во всех прочих библиотеках QSYSxxx вашей системы.
- Иногда в библиотеке System/38 встречаются команды, по своему действию эквивалентные той, которую вы собираетесь ограничить. Убедитесь, что вы ограничили доступ к эквивалентным командам в библиотеке QSYS38.
- Если вы работаете в среде System/36, то вам может потребоваться ограничить некоторые дополнительные программы. Например, программа QY2FTML в среде System/36 осуществляет передачу файлов.

Функции контроля за действиями

В этой главе 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. Обычно администратор защиты выполняет соответствующие действия регулярно. 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 безопасность 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 своевременного их аннулирования
  - Установка новых продуктов
- Для подготовки к выполнению определенной операции: установке нового приложения, повышению уровня защиты или настройке новой сети.

В этой главе описаны рекомендуемые действия для любой из перечисленных ситуаций. Выбор объектов для контроля и частота его проведения зависят от размера организации и требований к защите. В этой главе нет указаний по выбору частоты, с

которой следует выполнять действия по контролю; здесь даны ссылки на соответствующую информацию и перечислены способы ее получения и применения.

Этот раздел состоит из трех частей:

- Перечень объектов, действия над которыми можно контролировать.
- Информация о настройке и применении журнала контроля, предоставляемого системой.
- Информация о других способах сбора информации о защите в системе.

Контролирование действий заключается, помимо прочего, в применении команд и просмотре журналов и протоколов в системе iSeries. Для администратора, контролирующего действия, рекомендуется создать специальный пользовательский профайл. У этого профайла должны быть специальные права доступа *AUDIT, позволяющие изменять параметры защиты. Для выполнения некоторых задач контроля, описанных в этой главе, необходим пользовательский профайл со специальными правами доступа *ALLOBJ и *SECADM. По окончании периода контроля пароль профайла администратора защиты следует установить равным *NONE.

Дополнительная информация о контроле за действиями приведена в главе 9 книги *Security Reference*.

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 просмотра пользователей по профайлам групп:

```
      Показать пользователей с правами доступа

                        Последнее
Профайл      Пользоват. изменение  Пароль
группы       профайл    пароля    отсутств. Текст
DPTSM
             ANDERSOR   08/04/0x            Roger Anders
             VINCENTM   09/15/0x            Mark Vincent
DPTWH
             ANDERSOR   08/04/0x            Roger Anders
             WAGNERR    09/06/0x            Rose Wagner
QSECOFR
             JONESS     09/20/0x            Sharon Jones
             HARRISOK   08/29/0x            Ken Harrison
*NO GROUP
             DPTSM      09/05/0x    X       Sales and Marketing
             DPTWH      08/13/0x    X       Warehouse
             RICHARDS   09/05/0x            Janet Richards
             SMITHJ     09/18/0x            John Smith
```

Печать выбранных пользовательских профайлов

Команда Показать пользовательский профайл (DSPUSRPRF) позволяет создать файл вывода, который можно обработать с помощью утилиты Query.

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

Утилита Query позволяет создавать 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 создавать программы Query, которые будут выдавать 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 UPLTCP в модельном файле вывода базы данных, равно *NO или *PARTIAL).
- Список всех пользователей, у которых есть определенное начальное меню или начальная программа.
- Список неактивных пользователей (по дате последнего входа в систему).

Поиск больших пользовательских профайлов

Если в системе существует много пользовательских профайлов с широкими правами доступа, то выбранную стратегию защиты нельзя признать удачной. Ниже приведен способ обнаружения и проверки больших пользовательских профайлов.

1. Создайте файл вывода, содержащий информацию обо всех пользовательских профайлах системы с помощью команды Показать описание объекта (DSPOBJD):

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. Просмотрите список профайлов и их размеров, упорядоченный по убыванию размеров, с помощью программы Query.
3. Напечатайте подробную информацию о самых больших пользовательских профайлах и убедитесь в том, что права доступа и принадлежащие этим профайлам объекты выбраны правильно:

   ```
   DSPUSRPRF USRPRF(имя-пользовательского-профайла) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(имя-пользовательского-профайла) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Размер некоторых пользовательских профайлов фирмы 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.

Дополнительная информация о контроле защиты приведена в главе 9 книги *Security Reference*.

Анализ прав доступа к объектам

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)
   ```

Примечание: В выводе этой команды не указываются библиотеки из независимых пулов вспомогательной памяти, состояние которых отлично от AVAILABLE.

2. Просмотрите все права доступа к определенной библиотеке с помощью команды Показать права доступа к объекту (DSPOBJAUT):

   ```
   DSPOBJAUT OBJ(QSYS/имя-библиотеки) OBJTYPE(*LIB) +
             ASPDEV(имя-устройства-ASP) OUTPUT(*PRINT)
   ```

3. Просмотрите список объектов в библиотеке с помощью команды Показать библиотеку (DSPLIB):

   ```
   DSPLIB LIB(QSYS/имя-библиотеки) ASPDEV(имя-устройства-ASP) OUTPUT(*PRINT)
   ```

С помощью этих отчетов вы можете определить, какие объекты содержатся в библиотеке и какие пользователи имеют к ней доступ. При необходимости вы можете также просмотреть права доступа к выбранным объектам библиотеки с помощью команды DSPOBJAUT.

Поиск объектов с измененными атрибутами

Вы можете просмотреть список объектов с измененными атрибутами с помощью команды Проверить целостность объекта (CHKOBJITG). Наличие в системе объекта с измененными атрибутами обычно указывает на попытку несанкционированного доступа к системе. Эту команду рекомендуется запускать после каждого выполнения пользователями следующих операций в системе:

- Восстановление программ
- Применение Специальных сервисных средств (DST)

При применении этой команды система создает файл базы данных с информацией о возможных нарушениях целостности. Вы можете проверить объекты, принадлежащие одному профайлу, нескольким различным профайлам или всем профайлам. Вы можете выполнить поиск объектов с измененным атрибутом домена. Кроме того, вы можете заново вычислить контрольные значения программ, чтобы выполнить поиск объектов типа *PGM, *SRVPGM, *MODULE и *SQLPKG с измененными атрибутами.

Для применения команды CHKOBJITG необходимы специальные права доступа *AUDIT. Выполнение этой команды может занять много времени, поскольку при этом проводится много операций поиска и вычислений. Эту команду следует запускать только при низкой загруженности системы.

Примечание: Профайлы, которым принадлежит большое число объектов с широким набором частных прав доступа, могут быть очень велики. 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. **Не присваивайте все (или почти все) объекты одному пользовательскому профайлу.**

Анализ программ, принимающих права доступа

Программы, принимающие права доступа пользователя со специальными правами доступа *ALLOBJ, представляют угрозу для защиты. Определить и проверить такие программы 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 пользователей с правами доступа *ALLOBJ приведены в разделе “Печать выбранных пользовательских профайлов” на стр. 51.

2. Определите пользователей, у которых есть права на применение принимающих программ и общие права доступа к программам, с помощью команды DSPOBJAUT:

   ```
   DSPOBJAUT OBJ(имя-библиотеки/имя-программы) +
             OBJTYPE(*PGM) ASPDEV(библиотека/программа) +
             OUTPUT(*PRINT)
   ```

3. Проверьте исходный код программы и ее описание и с помощью этой информации определите:
   - Запрещен ли пользователю или программе, принимающим права доступа, доступ к ненужным им функциям, например к командной строке.
   - Достаточны ли принимаемые программой права доступа для выполнения необходимых действий. Приложения, применяющие сбой программы, 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(библиотека/программа) +
           DETAIL(*FULL)
   ```

Работа с журналом контроля и получателями журнала

Журнал контроля QSYS/QAUDJRN предназначен исключительно для контроля защиты. В нем не следует регистрировать объекты. Он также не должен использоваться при управлении фиксацией. Наконец, в него не следует отправлять пользовательские записи с помощью команды Отправить запись журнала (SNDJRNE) или API Отправить запись журнала (QJOSJRNE).

Занесение записей в журнал контроля осуществляется в специальном режиме блокировки. Если ведется контроль (системное значение QAUDCTL не равно *NONE), то системное задание-арбитр (QSYSARB) блокирует журнал QSYS/QAUDJRN. При ведении контроля вы можете выполнять над журналом контроля некоторые действия, например:

- Команда DLTJRN
- Команда ENDJRNxxx
- Команда APYJRNCHG
- Команда RMVJRNCHG
- Команда DMPOBJ или DMPSYSOBJ
- Перемещение журнала
- Восстановление журнала
- Действия над правами доступа, такие как команда GRTOBJAUT
- Команда WRKJRN

Записи защиты, заносимые в журнал контроля, описаны в книге *Security Reference*. Код всех записей защиты в журнале контроля равен T. Помимо записей защиты, журнал QAUDJRN содержит также 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 занести записи защиты, то действие системы в этом случае определяется системным значением QAUDENDACN. Поврежденный журнал контроля или его получатель следует восстанавливать так же, как обычный журнал или получатель.

Рекомендуется настроить автоматическую замену получателей журнала в системе. При создании журнала QAUDJRN укажите значение MNGRCV(*SYSTEM) или присвойте журналу это значение. 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**. Дополнительная информация приведена в iSeries Information Center—>Управление системами–> Работа с журналом–>Работа с локальным журналом–>Работа с журналами. Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Глава 6. Настройка прав доступа

Для отслеживания конфигурации прав доступа в вашей системе служит набор отчетов о защите. При первом запуске этих отчетов вы можете напечатать всю информацию, (права доступа ко всем файлам или всем программам, например).

После создания базы информации вы можете регулярно вызывать печать отчетов об изменениях. Отчеты об изменениях помогут вам отслеживать все выполненные в системе изменения в конфигурации защиты, которые требуют контроля с вашей стороны. Например, вы можете еженедельно вызывать печать отчета, в котором перечисляются общие права доступа к файлам. Можно запросить печать только информации об изменениях. В таком варианте отчета будут перечислены все новые файлы системы, доступные всем пользователям, а также существующие файлы, общие права доступа к которым были изменены с момента вызова последнего отчета.

Запуск средства защиты может осуществляться из двух меню:

- Меню SECTOOLS служит для интерактивного выполнения программ.
- Меню SECBATCH служит для выполнения программ в пакетном режиме. Это меню состоит из двух частей: одна предназначена для немедленной передачи задания в очередь, а вторая - для помещения заданий в планировщик заданий.

Для запуска средств защиты с помощью Навигатора iSeries выполните следующие действия:

1. В окне программы Навигатор iSeries разверните значок своего сервера—>**Защита**.
2. Щелкните правой кнопкой мыши на пункте **Стратегии** и выберите опцию **Просмотреть**. Появится список стратегий, которые можно создать или изменить.

Настройка общих прав доступа к объектам

Для упрощения работы и для повышения производительности во многих системах большинство объектов доступно большинству пользователей. Пользователя чаще явно запрещают доступ к отдельной конфиденциальной информации и объектам, вместо того, чтобы явно предоставлять доступ к каждому объекту. Но в некоторых системах с высокими требованиями к защите применяется обратный подход, и доступ к объектам разрешается по отдельности. В таких системах большинство объектов создается с общими правами доступа *EXCLUDE.

iSeries - это объектно-ориентированная система, в котором существуют объекты различных типов. Большинство типов объектов не содержат конфиденциальную информацию и не выполняют функций, связанных с защитой системы. Администраторы защиты системы iSeries со стандартными потребностями обычно уделяют основное внимание объектам, требующим защиты, например, файлам базы данных и программам. Для объектов других типов вы можете задать общие права доступа, достаточные для работы с приложениями. Обычно, это права доступа *USE.

С помощью команды Печатать общие права доступа (PRTPUBAUT) вы можете напечатать информацию об объектах, к которым имеют доступ непривилегированные пользователи. (**Непривилегированный пользователь** - это пользователь, у которого есть права на вход в систему, но у которого нет прав доступа к объекту, присвоенных явно). При вызове команды PRTPUBAUT вы можете указать конкретные типы объектов, а также библиотеки и каталоги для просмотра. В меню SECBATCH и SECTOOLS включены опции для печати отчета с информацией

об общедоступных объектах, которые обычно связаны с конфигурацией защиты системы. Вы можете регулярно печатать вариант этого отчета, содержащий только информацию об изменениях для того, чтобы отслеживать и контролировать действия, выполняемые над объектами.

Настройка прав доступа к новым объектам

В операционной системе OS/400 предусмотрены функции управления правами доступа и принадлежности новых объектов. При создании объекта пользователем система определяет следующее:

- Кто будет являться владельцем объекта
- Общие права к данному объекту
- Будут ли предоставлены частные права доступа к этому объекту
- Где будет расположен объект (в какой библиотеке или каталоге)
- Будет ли доступ к объекту контролироваться

Система определяет эти характеристики на основании системных значений, параметров библиотек и параметров пользовательских профайлов. В разделе “Присвоение прав доступа и принадлежности новым объектам” главы 5 в книге *iSeries Security Reference* приведено несколько примеров возможных вариантов.

С помощью команды PRTUSRPRF вы можете напечатать параметры пользовательского профайла, определяющие принадлежность и права доступа к новым объектам. На рис. 5 на стр. 63 приведен пример выводимого отчета.

Настройка списков прав доступа

С помощью списков прав доступа вы можете сгруппировать объекты по схожим требованиям к защите. В списке прав доступа перечислены пользователи и их права доступа к объектам, защищенным этим списком. Списки прав доступа предоставляют эффективный способ управления правами доступа к схожим объектам системы. Но в некоторых случаях их применение затрудняет отслеживание прав доступа к объектам.

С помощью команды Печатать общие права доступа (PRTPVTAUT) вы можете напечатать информацию о правах доступа, перечисленных в списке прав доступа. На рис. 3 показан пример выводимого отчета.

```
                    Частные права доступа (Полный отчет)
SYSTEM4
Список прав                  Основная                Права      List  ----------Объект-----------  ------------Данные----------
доступа       Владелец       группа    Пользователь  доступа    .Mgt   Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
LIST1         QSECOFR        *NONE        *PUBLIC    *EXCLUDE
LIST2         BUDNIKR        *NONE        BUDNIKR    *ALL        X     X    X     X      X     X    X     X    X    X      X
                                          *PUBLIC    *CHANGE           X                              X     X    X    X      X
LIST3         QSECOFR        *NONE        *PUBLIC    *EXCLUDE
LIST4         CJWLDR         *NONE        CJWLDR     *ALL        X     X    X     X      X     X    X     X    X    X      X
                                          GROUP1     *ALL              X    X     X      X     X    X     X    X    X      X
                                          *PUBLIC    *EXCLUDE
```

Рисунок 3. Отчет о частных правах доступа для списков прав доступа

В этом отчете показана та же информация, которую вы можете видеть в меню Редактировать список прав доступа (EDTAUTL). Преимущество отчета заключается в том, что здесь приведена информация о всех списках прав доступа одновременно. Например, если вы настраиваете защиту для новой группы объектов, вы можете быстро просмотреть отчет и проверить, не подходит ли для данных объектов какой-либо из существующих списков прав доступа.

Вы можете напечатать вариант этого отчета, содержащий только информацию об изменениях, выполненных с момента последнего запроса этого отчета. В нем будут перечислены только новые списки прав доступа или списки с измененными правами доступа. Вы можете также напечатать список объектов, защищенных каждым списком прав доступа. На рис. 4 показан пример такого отчета для одного списка прав доступа:

```
                    Показать объекты списка прав доступа
Список прав доступа. . . . . :   CUSTAUTL
Библиотека . . . . . :     QSYS
Владелец . . . . . :   AROWNER
Основная группа  . . . . . :   *NONE

                                                    Основная
Объект         Библиотека     Тип         Владелец  группа          Описание
CUSTMAS        CUSTLIB        *FILE       AROWNER   *NONE
CUSTORD        CUSTORD        *FILE       OEOWNER   *NONE
```

Рисунок 4. Показать отчет об объектах списка прав доступа

Этот отчет поможет вам, к примеру, определить результат добавления пользователя в список прав доступа (какие права доступа он при этом получит).

Работа со списками прав доступа

Средства защиты, предусмотренные в Навигаторе iSeries, помогут вам разработать план и стратегию защиты и настроить систему с учетом предъявляемых требований. В частности, при настройке защиты вы можете применять списки прав доступа.

Ниже описаны характеристики списков прав доступа.

- Списки прав доступа объединяют в группы объекты со схожими требованиями к защите.
- В списке прав доступа перечислены пользователи и их права доступа к объектам, защищенным этим списком.
- У каждого пользователя и группы пользователей могут быть свои права доступа к набору объектов, защищенных списком.
- Права доступа удобнее задавать списком, а не для каждого отдельного пользователя или группы пользователей.

Над списком прав доступа можно выполнить следующие действия:

- Создать список прав доступа
- Изменить список прав доступа
- Добавить пользователей или группы пользователей в список прав доступа
- Изменить права доступа пользователя
- Просмотреть защищенные списком объекты

Для работы со списком прав доступа выполните следующие действия:

1. В окне Навигатора iSeries разверните значок сервера—>Защита. Появятся пункты **Списки прав доступа** и **Стратегии**.
2. Щелкните правой кнопкой мыши на пункте **Списки прав доступа** и выберите опцию **Создать список прав доступа**. В окне **Создать список прав доступа** предусмотрены следующие варианты прав доступа.
   - **На использование:** Разрешить доступ к атрибутам объекта и использование объекта. Обычные пользователи могут просматривать, но не изменять объекты.

- **На изменение:** Разрешить изменение содержимого объекта (за некоторыми исключениями).
- **Все:** Разрешить выполнение всех действий над объектом, за исключением тех, которые разрешены только его владельцу. Пользователь или группа пользователей могут управлять существованием объекта, настраивать его защиту, изменять объект и выполнять над ним основные действия. Пользователь или группа могут также изменять принадлежность объекта.
- **Нет:** Запретить выполнение любых действий над объектом. Пользователи и группы с такими правами доступа не могут обращаться к объекту и выполнять над ним какие-либо действия. Этот пункт означает, что пользователям с правами *PUBLIC запрещено использование объекта.

При работе со списками прав доступа вы можете предоставлять доступ как к объектам, так и к данным. Ниже перечислены права доступа к объектам, которые вы можете предоставить.

- **Операционные:** Позволяют просмотреть описание объекта и использовать объект в соответствии с правами доступа к данным объекта.
- **На управление:** Позволяют задавать конфигурацию защиты объекта, переименовывать или перемещать объект и добавлять элементы в файлы базы данных.
- **К существованию:** Позволяют управлять существованием и принадлежностью объекта. Пользователь или группа пользователей могут удалять объект, освобождать занимаемую объектом память, сохранять и восстанавливать объект и передавать объект другому владельцу. Если у пользователя или группы есть специальные права на сохранение объекта, им не нужны права к существованию объекта.
- **На изменение атрибутов** (применяются только к файлам баз данных и пакетам SQL): Позволяют изменять атрибуты объекта. Если у пользователя или группы пользователей есть такие права доступа к файлу базы данных, они могут добавлять и удалять триггеры, добавлять и удалять ограничения уникальности и ограничения по ссылкам, а также изменять атрибуты файла базы данных. Если у пользователя или группы есть такие права доступа к пакету SQL, то пользователь или группа могут изменять атрибуты пакета SQL. В настоящее время такие права доступа применяются только к файлам баз данных и пакетам SQL.
- **На обращение к объекту** (применяются только к файлам баз данных и пакетам SQL): Позволяют ссылаться на объект из другого объекта, причем последний может ограничить набор действий, выполняемых над данным объектом. Если у пользователя или группы пользователей есть такие права доступа к физическому файлу, то пользователь или группа могут добавлять ограничения по ссылкам, для которых физический файл будет родительским. В настоящее время такие права доступа применяются только к файлам баз данных.

Ниже перечислены права доступа к данным, которые вы можете предоставить.

- **На чтение:** Позволяют получить и просмотреть содержимое объекта, например, просмотреть записи в файле.
- **На добавление:** Позволяют добавлять записи в объект, например, сообщения в очередь сообщений или записи в файл.
- **На обновление:** Позволяют изменять записи объектов, например, записи в файлах.
- **На удаление:** Позволяют удалять записи из объектов, например, сообщения из очереди сообщений или записи из файла.
- **На выполнение:** Позволяют запускать программы, служебные программы или пакеты SQL. Пользователь с такими правами доступа может также помещать объекты в библиотеки или каталоги.

Дополнительная информация о создании и изменении списков прав доступа приведена в электронной справке программы Навигатор iSeries.

Просмотр стратегий в Навигаторе iSeries

Навигатор iSeries позволяет просмотреть и изменить стратегии, настроенные для сервера iSeries. В Навигаторе iSeries предусмотрено пять типов стратегий:

- **Стратегия контроля**
  Позволяет задать параметры сбора данных об отдельных действиях и обращениях к определенным ресурсам системы.
- **Стратегия защиты**
  Позволяет задать уровень защиты системы и другие параметры защиты.
- **Стратегия паролей**
  Позволяет задать уровень паролей, применяемых в системе.
- **Стратегия восстановления**
  Позволяет задать способ восстановления различных объектов системы.
- **Стратегия входа в систему**
  Позволяет задать параметры входа в систему.

Для просмотра или изменения стратегий с помощью Навигатора iSeries выполните следующие действия:

1. В окне программы Навигатор iSeries разверните значок сервера—>**Защита**.
2. Щелкните правой кнопкой мыши на пункте **Стратегии** и выберите опцию **Просмотреть**. Появится список стратегий, которые можно создать или изменить. Более подробная информация о различных стратегиях приведена в электронной справке программы Навигатор iSeries.

Настройка частных прав доступа к объектам

Опции меню SECBATCH:
12 - *Передать на выполнение немедленно* **41** - *Поместить в планировщик заданий*

Команда Печатать частные права доступа (PRTPVTAUT) служит для вывода списка всех частных прав доступа к объектам указанного типа в указанной библиотеке.

С помощью этого отчета вы можете выявить новые права доступа к объектам. Эта информация поможет вам также следить за правильностью схемы частных прав доступа и предотвратить возникновение в ней противоречий.

Ограничение доступа к очередям вывода и очередям заданий

Некоторые администраторы защиты выполняют большую работу по защите доступа к файлам, забывая при этом, что происходит при печати содержимого файлов. На сервере iSeries предусмотрены функции для защиты очередей вывода и очередей заданий. Можно задать защиту очереди вывода так, что пользователи без соответствующих прав доступа не смогут, например, просматривать или копировать конфиденциальные буферные файлы, находящиеся в очереди на печать. Для очереди заданий можно задать такую защиту, что пользователи без соответствующих прав доступа не смогут перенаправить задание в ненастроенную очередь заданий или отменить его выполнение.

Опции меню SECBATCH:
24 - *передать на выполнение немедленно*, **63** - *поместить в планировщик заданий*

В разделе *Basic system security and planning* справочной системы Information Center и в книге *iSeries Security Reference* описано, как установить защиту очередей вывода и очередей заданий.

С помощью команды Печатать права доступа к очереди (PRTQAUT) вы можете напечатать настройки защиты для очередей ввода и очередей заданий в вашей системе. После этого вы сможете изучить процесс печати заданий с конфиденциальной информацией и убедиться, что эти задания направляются в защищенные очереди заданий и очереди вывода.

Вы можете сравнить параметры защиты, установленной вами для очередей вывода и очередей заданий, с данными в Приложении D книги *iSeries Security Reference*. В приведенных в этом приложении таблицах указано, какие установки требуются для выполнения различных функций над очередями вывода и очередями заданий.

Настройка специальных прав доступа

Все усилия по созданию грамотной схемы прав доступа к объектам могут пропасть зря, если окажется, что у пользователей системы есть специальные права доступа, которые не требуются им для работы. Нет смысла задавать права доступа к объектам, если пользователь обладает специальными правами доступа *ALLOBJ. Если же у пользователя есть специальные права доступа *SPLCTL, то он может просматривать любой буферный файл, независимо от того, защищена ли очередь, в которую он помещен. Пользователь со специальными правами *JOBCTL может управлять системными операциями и перенаправлять задания. Специальные права *SERVICE предоставляют доступ к данным через служебные средства без взаимодействия с операционной системой.

Опции меню SECBATCH:
29 - *передать на выполнение немедленно*, **68** - *поместить в планировщик заданий*

С помощью команды Печатать пользовательский профайл (PRTUSRPRF) вы можете напечатать информацию о специальных правах доступа и о классе пользователей для пользовательского профайла вашей системы. Существует несколько опций вывода этого отчета:
- Все пользовательские профайлы
- Пользовательские профайлы с конкретными специальными правами доступа
- Пользовательские профайлы с конкретными классами пользователей
- Пользовательские профайлы, в которых наблюдаются несоответствия между классом пользователя и специальными правами доступа.

На рис. 5 на стр. 63 показан пример отчета, в котором показаны специальные права доступа для всех пользовательских профайлов:

```
                                   Информация о пользовательском профайле
  Тип отчета   . . . . . . . . . :   *AUTINFO
  Критерий выбора. . . . . . . . :   *SPCAUT
  Специальные права доступа. . . :   *ALL
                   ----------Специальные права доступа----------
                                *IO                                                    Группа
Польз.    Профайлы  *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Класс            Права доступа  Тип прав   Ограничение
профайл   групп      OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  пользов   Владелец  группы       доступа    возможностей
USERA     *NONE      X     X     X    X     X     X     X     X    *SECOFR   *USRPRF   *NONE        *PRIVATE   *NO
USERB     *NONE                      X     X                       *PGMR     *USRPRF   *NONE        *PRIVATE   *NO
USERC     *NONE      X     X     X    X     X     X     X     X    *SECOFR   *USRPRF   *NONE        *PRIVATE   *NO
USERD     *NONE                                                    *USER     *USRPRF   *NONE        *PRIVATE   *NO
```

Рисунок 5. Отчет с информацией о пользователях: Пример 1

Помимо специальных прав доступа в этом отчете показана следующая информация:

- Ограничены ли возможности данного пользовательского профайла.
- Является ли данный пользователь (или его группа) владельцем создаваемых им объектов.
- Какие права доступа к создаваемым данным пользователем объектам автоматически присваиваются группе пользователя.

На рис. 6 показан пример отчета с информацией о несовпадениях специальных прав доступа и классов пользователей:

```
Информация о пользовательском профайле
Тип отчета   . . . . . . . . . :   *AUTINFO
Критерий выбора. . . . . . . . :   *MISMATCH
--------------------------------Специальные права доступа--------
                                *IO                                                    Группа
Польз.    Профайлы  *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Класс            Права доступа  Тип прав   Ограничение
профайл   групп      OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  пользов   Владелец  группы       доступа    возможностей
USERX     *NONE       X                X     X                 X    *SYSOPR   *USRPRF   *NONE        *PRIVATE    *NO
USERY     *NONE                                    X                *USER     *USRPRF   *NONE        *PRIVATE    *NO
USERZ                                              X                *USER     *USRPRF   *NONE        *PRIVATE    *NO
          QPGMR                        X     X
```

Рисунок 6. Отчет с информацией о пользователях: Пример 2

Обратите внимание в рис. 6 на следующее:

- Профайл USERX относится к классу ″системный оператор″ (*SYSOPR), но при этом обладает специальными правами доступа *ALLOBJ и *SPLCTL.
- Профайл USERY относится к классу ″пользователь″ (*USER), но обладает специальными правами доступа *SECADM.
- Профайл USERZ также относится к классу ″пользователь″ (*USER), но обладает специальными правами доступа *SECADM. USERZ является также элементом группы QPGMR, у которой есть специальные права доступа *JOBCTL и *SAVSYS.

Вы можете регулярно запрашивать такой отчет для отслеживания администрирования пользовательских профайлов.

Настройка параметров среды пользователя

Одно из назначений пользовательского профайла - определять параметры среды для пользователя, включающие в себя очередь вывода, начальное меню и описание задания. Среда пользователя определяет, как будет выглядеть система для пользователя и, в некоторой степени, что ему разрешено в системе. Пользователь должен обладать правами доступа к объектам, указанным в его пользовательском профайле. Но в том случае, если схема прав доступа еще находится в процессе

разработки или если она не накладывает строгих ограничений, среда, определенная в пользовательском профайле, может приобрести нежелательные свойства. Ниже приведено несколько примеров:

Опции меню SECBATCH:

29 - *Передать на выполнение немедленно* **68** - *Поместить в планировщик заданий*

- В описании задания пользователя может быть указан пользовательский профайл с большими правами доступа, чем у данного пользователя.
- Для пользователя может быть задано начальное меню, не содержащее командную строку. Но может оказаться, что программа обработки клавиши Attention предоставляет ему доступ к командной строке.
- Пользователю может быть разрешено запрашивать конфиденциальные отчеты. Но вывод этого пользователя может направляться в очередь вывода, доступную и другим пользователям, которые не должны иметь доступа к этим отчетам.

С помощью опции *ENVINFO команды Печатать пользовательский профайл (PRTUSRPRF) вы можете отслеживать свойства операционных сред, определенных для пользователей системы. На рис. 7 показан пример вывода этой команды:

```
                                  Информация о пользовательском профайле
  Тип отчета  . . . . . . . . . :   *ENVINFO
  Критерий выбора. . . . . . . :   *USRCLS
                        Начальное      Начальная      Описание       Очередь        Очередь        Программа
Пользоват.    Текущая   меню/          программа/     задания/       сообщений/     вывода/        Attention/
профайл       библиотека Библиотека     Библиотека     Библиотека     Библиотека     Библиотека     Библиотека
AUDSECOFR     AUDITOR    MAIN           *NONE           QDFTJOBD      QSYSOPR        *WRKSTN        *SYSVAL
                         *LIBL                          QGPL           QSYS
USERA         *CRTDFT    OEMENU         *NONE           QDFTJOBD      USERA          *WRKSTN        *SYSVAL
                         *LIBL                          QGPL           QUSRSYS
USERB         *CRTDFT    INVMENU        *NONE           QDFTJOBD      USERB          *WRKSTN        *SYSVAL
                         *LIBL                          QGPL           QUSRSYS
USERC         *CRTDFT    PAYROLL        *NONE           QDFTJOBD      USERC          PAYROLL        *SYSVAL
                         *LIBL                          QGPL           QUSRSYS         PRPGMLIB
```

Рисунок 7. Пример вывода команды Печатать пользовательский профайл - Среда пользователя

Применение сервисных средств

Сервисные средства служат для настройки и обслуживания сервера, а также для управления им. Для работы с сервисными средствами применяются функции Специальные сервисные средства (DST) и Системный инструментарий (SST). При обращении к DST, SST или функциям Навигатора iSeries, предназначенным для работы с логическими разделами (LPAR) и диском, требуется задать ИД пользователя сервисных средств.

Функцию DST можно вызвать после загрузки Лицензионного внутреннего кода, когда операционная система OS/400 еще не загружена. Функцию SST можно вызвать из операционной системы OS/400. В приведенной ниже таблице перечислены основные различия между DST и SST.

Свойство	DST	SST

Способ запуска	Можно запустить с консоли при выполнении IPL вручную, либо с панели управления, выбрав опцию 21.	Можно запустить в интерактивном задании, при условии, что есть права доступа QSRV или следующие права доступа: • Права на выполнение команды CL STRSST (Запустить SST). • Служебные права доступа (*SERVICE) или права доступа ко всем объектам (*ALLOBJ). • Права на применение функции SST.
Когда доступна	Функция доступна даже в том случае, если сервер работает в режиме с ограничениями. Для работы с DST операционная система OS/400 не требуется.	Функция доступна в том случае, если запущена операционная система OS/400. OS/400 необходима для работы с SST.
Способ идентификации	Требуется задать ИД и пароль пользователя сервисных средств.	Требуется задать ИД и пароль пользователя сервисных средств.

В разделе iSeries Information Center—>Защита—>Сервисные средства можно найти информацию о выполнении следующих задач:

- Работа с сервисными средствами с помощью функции DST
- Работа с сервисными средствами с помощью функции SST
- Работа с сервисными средствами с помощью Навигатора iSeries
- Создание ИД пользователя сервисных средств
- Изменение прав доступа пользователя сервисных средств
- Изменение описания пользователя сервисных средств
- Просмотр ИД пользователя сервисных средств
- Подключение и отключение ИД пользователя сервисных средств
- Удаление ИД пользователя сервисных средств
- Изменение ИД и пароля пользователя сервисных средств с помощью SST или DST
- Изменение своего пароля пользователя сервисных средств с помощью команды STRSST
- Изменение ИД и пароля пользователя сервисных средств с помощью
- API Изменить ИД пользователя сервисных средств (QSYCHGDS)
- Сброс пароля пользовательского профайла QSECOFR в OS/400
- Сброс ИД и пароля профайла QSECOFR в сервисных средствах
- Сохранение и восстановление параметров защиты, заданных в сервисных средствах
- Создание собственной версии ИД пользователя сервисных средств профайла QSECOFR
- Настройка сервера сервисных средств для DST
- Настройка сервера сервисных средств для OS/400
- Контроль за применением служебных функций в DST
- Контроль за применением сервисных средств с помощью протокола контроля за действиями OS/400

Информация о работе со справочной системой iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Глава 7. Применение функции защиты логических разделов (LPAR)

На сервере iSeries рекомендуется создать несколько логических разделов в следующих случаях.

- **Работа с несколькими независимыми системами**: Вы можете логически изолировать программное обеспечение, выделив разделу часть системных ресурсов, таких как дисковые накопители, процессоры, память и устройства ввода-вывода. При правильной настройке логических разделов достигается также некоторая устойчивость системы к аппаратным сбоям. Вы можете изолировать друг от друга плохо совместимые пакетные и интерактивные задания, запустив их в разных логических разделах.
- **Объединение** : Система с логическими разделами может заменить несколько серверов iSeries. Вместо нескольких систем вы можете использовать одну систему с логическими разделами. Это позволит вам обойтись без затрат на дополнительное оборудование. При необходимости вы можете перераспределить ресурсы между логическими разделами.
- **Создание смешанной рабочей и тестовой среды:** С помощью логических разделов можно объединить рабочую и тестовую среду. Вы также можете создать раздел только с рабочей средой в основном разделе. Дополнительная информация о среде с несколькими рабочими разделами приведена ниже в главе *Создание нескольких рабочих разделов*.

  Логический раздел может быть либо тестовым, либо рабочим. В рабочем разделе запускаются все деловые приложения. Сбой в рабочем разделе может негативно отразиться на выполнении деловых операций и привести к потере времени и денег. Тестовый раздел предназначен для тестирования программного обеспечения. Сбой в тестовом разделе не повлияет на выполнение повседневных деловых операций.
- **Создание нескольких рабочих разделов:** Если в системе есть несколько рабочих разделов, то их роль должны играть дополнительные разделы. В этом случае основной раздел выделяется для управления разделами.
- **Оперативное сохранение:** Если резервная копия дополнительного раздела будет создана в другом разделе той же системы, то в случае сбоя вы сможете минимизировать его последствия, переключившись на резервный раздел. Кроме того, такая конфигурация позволяет максимально снизить продолжительность сохранения. Вы можете отключить резервный раздел и сохранить его, продолжая работу с другими разделами в обычном режиме. Однако для применения такой стратегии оперативного сохранения необходимо специальное программное обеспечение.
- **Интегрированный кластер:** С помощью OptiConnect/400 и программного обеспечения с высокой степенью готовности вы можете настроить систему для работы в режиме интегрированного кластера. Интегрированный кластер позволяет защитить систему от неожиданных сбоев в дополнительном разделе.

Примечание: При настройке дополнительного раздела необходимо обратить особое внимание на набор карт. Если процессор ввода-вывода (IOP), выбранный для консоли, содержит карту LAN, но последняя не предназначена для работы с Консолью управления, то карта будет использоваться консолью, и вы не сможете применять ее в своих целях. Дополнительная информация по работе с Консолью управления приведена в разделе Глава 8, “Консоль управления iSeries”, на стр. 71.

Дополнительная информация приведена в разделе ″Логические разделы″ справочной системы iSeries Information Center.

Управление защитой логических разделов

Для защиты системы с логическими разделами вы можете предпринять те же действия, что и для защиты системы без логических разделов. Однако учтите, что в случае логических разделов вам приходится работать с несколькими независимыми системами. Таким образом, вам необходимо будет выполнить одни и те же действия по защите для каждого отдельного логического раздела.

При настройке защиты логических разделов необходимо помнить и соблюдать следующие рекомендации и правила:

- Не добавляйте учетные записи пользователей одновременно в разные логические разделы. Добавляйте учетные записи только в тот раздел, доступ к которому необходимо предоставить.
- Ограничьте число пользователей основного раздела с правом доступа к Специальным сервисным средствам (DST) и Системному инструментарию (SST). Дополнительная информация о DST и SST приведена в разделе ″Управление логическими разделами с помощью Навигатора iSeries, DST и SST″ в iSeries Information Center. Дополнительная информация об управлении доступом к разделу с помощью пользовательских профайлов приведена в разделе “Применение сервисных средств” на стр. 64.

  Примечание: Для работы с функциями LPAR с помощью Навигатора iSeries необходимо запустить Сервер сервисных средств (STS). Более подробная информация приведена в iSeries Information Center—>Защита—>Сервисные средства. Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.
- Дополнительным разделам абсолютно недоступны оперативная память и диски других логических разделов.
- Дополнительным разделам доступны только их собственные аппаратные ресурсы.
- Из основного раздела можно просмотреть все аппаратные ресурсы системы с помощью меню DST или SST Работа с разделами системы.
- Операционной системе основного раздела доступны только аппаратные ресурсы основного раздела.
- Панель управления системой позволяет управлять основным разделом. Если панель работает в режиме Secure, то выполнить какие-либо действия с помощью меню SST Работа с состоянием раздела невозможно. Для того чтобы подключить DST с панели управления, необходимо перевести систему в режим Manual.
- При переключении дополнительного раздела в режим Secure вы можете ограничить применение меню Работа с состоянием раздела следующими способами:
  - Разрешить изменение состояния дополнительного раздела только с помощью DST, но не SST.
  - Разрешить запуск DST в дополнительном разделе только из основного раздела, из меню DST или SST Работа с состоянием раздела.
  - Переключать дополнительный раздел из состояния Secure в любое другое только с помощью DST основного раздела.

Если дополнительный раздел не находится в состоянии Secure, то его состояние можно изменять, запуская на нем как DST, так и SST.

Дополнительная информация о защите сервера iSeries приведена в книге Security Reference и разделе iSeries Information Center, посвященном защите системы и планированию стратегии защиты.

Глава 8. Консоль управления iSeries

Консоль управления позволяет управлять работой сервера iSeries с персонального компьютера. В частности, она позволяет удаленному PC установить соединение с сервером iSeries без применения консоли. В этом случае удаленный PC сам играет роль консоли. При работе с Консолью управления следует обратить внимание на следующее:

- Консоль управления позволяет выполнять те же задачи, что и обычная консоль. Например, пользователи со специальными правами доступа *SERVICE или *ALLOBJ могут запустить сеанс Консоли управления, даже если эти пользователи отключены.
- Консоль управления устанавливает соединение с сервером iSeries с помощью пользовательских профайлов и паролей сервисных средств. Поэтому крайне важно изменить пользовательские профайлы и пароли сервисных средств. Если вы оставите пользовательские профайлы и пароли по умолчанию, то, используя их, хакеры смогут установить соединение между удаленной консолью и сервером iSeries. Советы по настройке паролей приведены в разделах “Изменение стандартных паролей” на стр. 20 и “Изменение паролей по умолчанию” на стр. 26.
- Защитить информацию при работе с Удаленной консолью позволяет опция ответного звонка Удаленного доступа к сети Windows.
- При настройке дополнительного раздела необходимо уделить особое внимание расположению карт. Если к выбранному процессору ввода-вывода (IOP) подключена сетевая карта, которая не предназначена для применения с Консолью управления, то эта карта будет активизирована консолью, и использовать ее в других целях будет невозможно.

В версии V5R1 Консоль управления была усовершенствована и теперь может применяться в локальной сети (LAN). Улучшенные процедуры идентификации и шифрования данных обеспечивают защиту операций консоли в сети. Для работы с Консолью управления в локальной сети настоятельно рекомендуется установить следующие программные продукты:

- Продукт Cryptographic Access Provider, 5722–AC2 или 5722–AC3 - на сервере iSeries
- Client Encryption, 5722–CE2 или 5722–CE3 - на PC с Консолью управления

Для шифрования данных консоли на сервере iSeries должен быть установлен один из продуктов Cryptographic Access Provider, **а** на персональном компьютере - один из продуктов Client Encryption.

Примечание: Если программы шифрования не установлены, шифрование данных не выполняется.

Приведенная ниже таблица содержит обзор способов шифрования, применяемых в существующих продуктах:

Таблица 13. Способы шифрования

Cryptographic Access Provider на сервере iSeries	**Client Encryption на PC с Консолью управления**	**Способ шифрования данных**
Нет	Нет	Нет
5722–AC2	5722–CE2	56-разрядное
5722–AC2	5722–CE3	56-разрядное

Таблица 13. Способы шифрования (продолжение)

Cryptographic Access Provider на сервере iSeries	Client Encryption на PC с Консолью управления	Способ шифрования данных
5722–AC3	5722–CE2	56-разрядное
5722–AC3	5722–CE3	128-разрядное

Дополнительная информация о настройке и применении Консоли управления iSeries приведена в справочной системе iSeries.

Защита Консоли управления - Обзор

Для защиты Консоли управления необходимо обеспечить следующее:

- идентификацию консоли
- идентификацию пользователя
- конфиденциальность данных
- целостность данных

Консоль управления с прямым соединением обеспечивает неявную идентификацию устройств и конфиденциальность и целостность данных за счет двухточечного соединения. Вход в меню консоли защищен с помощью процедуры идентификации пользователя.

Идентификация консоли

Процедура идентификации консоли предназначена для обнаружения консоли среди физических устройств. Консоль управления с прямым соединением применяет физическое соединение, напоминающее соединение твинаксиальной консоли. По этой причине физическая защита консоли может быть организована так же, как и в случае твинаксиальной консоли.

В Консоли управления с соединением LAN применяется одна из версий протокола Secure Sockets Layer (SSL), поддерживающая идентификацию устройства и пользователя без применения сертификатов. В этой версии идентификация устройства основана на профайле устройства сервисных средств. Подробные сведения приведены в разделе 73.

Идентификация пользователя

Идентификация пользователя предназначена для выяснения личности пользователя консоли. Процедура идентификации пользователя не зависит от типа консоли.

Конфиденциальность данных

Обеспечение конфиденциальности данных означает защиту данных от несанкционированного просмотра. Защита данных Консоли управления при прямом соединении обеспечивается с помощью физического соединения, схожего с твинаксиальным, а при соединении LAN - с помощью защищенного сетевого соединения. Способы обеспечения конфиденциальности данных в Консоли управления с прямым соединением и в твинаксиальном соединении схожи. Данные защищены физическим соединением.

Если установлены программы шифрования (ACx или CEx), то в Консоли управления с соединением LAN применяется защищенное сетевое соединение. В сеансе консоли применяется максимальный уровень шифрования, поддерживаемый программами шифрования на сервере iSeries и PC с Консолью управления.

Примечание: Если программы шифрования не установлены, шифрование данных не выполняется.

Целостность данных

Обеспечение целостности данных означает защиту данных от изменения на их пути к получателю. Защита данных Консоли управления при прямом соединении обеспечивается с помощью физического соединения, схожего с твинаксиальным, а при соединении LAN - с помощью защищенного сетевого соединения. Способы обеспечения целостности данных в Консоли управления с прямым соединением и в твинаксиальном соединении схожи. Данные защищены физическим соединением.

Если установлены программы шифрования (ACx или CEx), то в Консоли управления с соединением LAN применяется защищенное сетевое соединение. В сеансе консоли применяется максимальный уровень шифрования, поддерживаемый программами шифрования на сервере iSeries и PC с Консолью управления.

Примечание: Если программы шифрования не установлены, шифрование данных не выполняется.

Консоль управления с соединением LAN

Примечание: В качестве консоли может выступать любое устройство Консоли управления, однако пользовательский профайл сервисных средств применяется только в конфигурации на основе локальной сети.

На сервере iSeries по умолчанию заданы профайл устройства сервисных средств QCONSOLE и пароль QCONSOLE. Консоль управления с соединением LAN изменяет пароль после каждого успешного подключения. Дополнительная информация приведена в разделе “Работа с мастером настройки Консоли управления”.

Дополнительная информация о Консоли управления iSeries с соединением LAN приведена в соответствующем разделе Information Center.

Защита Консоли управления с соединением LAN

При работе с Консолью управления с соединением LAN рекомендуется выполнить следующие действия:

- Создайте дополнительный профайл устройства сервисных средств с атрибутами консоли и сохраните его в надежном месте.
- Установите продукт Cryptographic Access Provider, 5722–AC2 или 5722–AC3 на сервере iSeries и продукт Client Encryption, 5722–CE2 или 5722–CE3 на PC с Консолью управления.
- Задайте нетривиальный пароль для информации о сервисном устройстве.
- Обеспечьте защиту PC с Консолью управления таким же образом, как в случае твинаксиальной консоли или Консоли управления с прямым соединением.

Работа с мастером настройки Консоли управления

При настройке Консоли управления с соединением LAN Мастер настройки добавит необходимую информацию на персональный компьютер. Мастер настройки запрашивает профайл устройства сервисных средств, пароль этого профайла и пароль для защиты информации профайла устройства сервисных средств.

Примечание: Пароль информации профайла устройства сервисных средств предназначен для защиты этой информации (профайла устройства сервисных средств и его пароля) на персональном компьютере.

При установлении сетевого соединения Мастер настройки Консоли управления запросит пароль информации профайла устройства сервисных средств. Этот пароль необходим для доступа к зашифрованным профайлу устройства сервисных средств и паролю. Кроме того, Мастер настройки запросит идентификатор пользователя сервисных средств и пароль.

Глава 9. Выявление подозрительных программ

Ставшие популярными в последнее время направления использования компьютера увеличили вероятность попадания в вашу систему программ из непроверенных источников или программ, выполняющих неизвестные действия. Вот некоторые примеры:

- Пользователь персонального компьютера иногда получает программы от других пользователей PC. Если этот PC подключен к системе iSeries, то полученные программы могут повлиять на работу этой системы.
- Пользователи, подключенные к сетям, могут также принимать программы из разных источников, например с электронной доски объявлений.
- ″Взломщики″ систем стали более активны и технически оснащены. Они часто публикуют свои методы взлома и результаты. Эти методы могут взять на вооружение и другие, менее опытные программисты.

Все эти тенденции приводят к необходимости защиты компьютера от так называемых **компьютерных вирусов**. Вирус - это программа, которая встраивает свой код в код других программ. Такие программы называются ″зараженными вирусом″. Помимо этого вирусы могут выполнять другие операции, которые захватывают ресурсы системы или разрушают данные.

В архитектуре сервера iSeries предусмотрены средства защиты от компьютерных вирусов. Подробная информация приведена в разделе “Защита от компьютерных вирусов”. Администратор защиты сервера iSeries должен быть хорошо осведомлен о программах, которые могут выполнять несанкционированные действия. В дальнейших разделах данной главы описаны способы, которыми злоумышленники могут поместить в вашу систему вредоносные программы. В этих разделы приведены также советы по ограждению вашей системы от действия таких программ.

Совет по организации защиты

Права доступа к объектам - это главное средство защиты вашей системы. Если вы не составили четкий план защиты объектов, то ваша система уязвима. В данном разделе приведена информация о том, каким образом пользователь может обойти ограничения, которые накладываются на его действия схемой прав доступа к объектам, если в ней есть слабые места.

Защита от компьютерных вирусов

Наличие вируса в компьютере означает, что в нем хранится программа, которая может изменять код других программ. В объектно-ориентированной архитектуре iSeries злоумышленнику сложнее внедрить и распространить свой вирус, чем в других архитектурах. На сервере iSeries для работы с каждым типом объектов применяется свой набор команд и инструкций. Нельзя применить инструкцию для работы с файлом для того, чтобы изменить объект рабочей программы (а именно так действует большинство вирусов). Непросто также создать программу, которая изменяла бы объект другой программы. Это потребует много времени, усилий и навыков, при этом окажется необходим доступ к инструментам и документации, которые чаще всего недоступны.

С появлением функций, предназначенных для работы в среде открытых систем, на сервере iSeries перестали применяться некоторые функции защиты объектов. Например, в интегрированной файловой системе (IFS) пользователи могут напрямую работать с некоторыми объектами в каталоге, например, потоковыми файлами.

Хотя архитектура сервера iSeries препятствует распространению вирусов в программах сервера, сам сервер может являться ″переносчиком″ вируса. Например, если сервер iSeries применяется в качестве файлового сервера, то он хранит программы, которые используются многими пользователями PC. Любая из этих программ может содержать вирус, не обнаруженный сервером iSeries. Для предотвращения заражения подключенных к системе персональных компьютеров подобным способом, рекомендуется применять антивирусное программное обеспечение.

На сервере iSeries предусмотрено несколько функций, позволяющих защитить рабочие объекты программ от их изменения с помощью указателей, поддерживаемых в языках программирования низкого уровня:

- Если в вашей системе установлен уровень защиты 40 и выше, то защита целостности включает в себя средства против изменения объектов программ. Например, вы не можете успешно запустить программу, содержащую блокированные (защищенные) машинные инструкции.
- Контрольное значение программы также обеспечивает дополнительную защиту при восстановлении программы, сохраненной (и, возможно, измененной) в другой системе. В главе 2 книги *iSeries Security Reference* описаны функции защиты целостности для уровня защиты 40 и выше, включая информацию о контрольных значениях программ.

  Примечание: Контрольное значение программ не защищено от ошибочного использования и его применение не отменяет необходимость проверять программы, восстанавливаемые в системе.

Для отслеживания появления в вашей системе измененных программ существует еще несколько средств:

- С помощью команды Проверить целостность объекта (CHKOBJITG) вы можете исследовать объекты (рабочие объекты), найденные по указанным критериям, и определить, были ли они изменены. Действие этой команды похоже на работу функции поиска вирусов.
- Для отслеживания измененных или восстановленных программ вы можете также вызывать функцию контроля защиты. Установки *PGMFAIL, *SAVRST и *SECURITY системного значения Уровень прав доступа предоставляют записи контроля, с помощью которых вы можете выявить попытки записи в вашу систему программы-вируса. В главе 9 и приложении F книги *iSeries Security Reference* приведена дополнительная информация о значениях контроля и записях журнала контроля.
- С помощью параметра Принудительное создание (FRCCRT) команды Изменить программу (CHGPGM) вы можете повторно создать любую программу, которая была восстановлена в системе. Для этого система применяет шаблон программы. Если объект программы был изменен после компиляции, то система заново создаст и заменит измененный объект. Если шаблон программы содержит заблокированные (запрещенные) инструкции, система не создаст программу повторно.
- С помощью системного значения QFRCCVNRST (Преобразование при восстановлении) можно указать, что во время восстановления должны заново

создаваться все программы. Для повторного создания программы применяется ее шаблон. С помощью системных значений можно указать, какие программы должны создаваться заново.

- Системное значение QVFYOBJRST (Проверять объекты при восстановлении) позволяет запретить восстановление программ, у которых цифровая подпись отсутствует или неверна. Неверная цифровая подпись означает, что программа была изменена после того, как была подписана разработчиком. Вы можете подписывать свои программы, файлы сохранения и потоковые файлы с помощью специальных API.

Дополнительная информация о цифровых подписях объектов и защите системы с их помощью приведена в разделе “Создание подписей объектов” на стр. 88.

Отслеживание применения принятых прав доступа

На сервере iSeries можно создать программу, которая принимает права доступа своего владельца. Это означает, что любой пользователь, запустивший эту программу, получает такие же права доступа (частные и специальные), которые предоставлены пользовательскому профайлу-владельцу программы.

При правильном использовании принимаемые права доступа являются хорошим средством защиты. К примеру, в разделе “Дополнение возможностей системы меню средствами защиты объектов” на стр. 47 описано, как, сочетая возможности принимаемых прав доступа и системы меню, повысить эффективность работы с управлением доступом через меню. С помощью принятых прав доступа вы можете запретить изменение важных файлов без использования проверенных приложений, не запрещая при этом запросы к этим файлам.

Администратор защиты должен проверять правильность применения принимаемых прав доступа:

- Программы должны принимать права доступа только от тех пользовательских профайлов, которым предоставлены достаточные для выполнения необходимых функций, но не избыточные права доступа. Особенно внимательно следует отслеживать программы, принимающие права доступа от профайла, который обладает специальными правами доступа *ALLOBJ или является владельцем важных объектов.
- Программы, принимающие права доступа, должны выполнять точно определенные, ограниченные функции и не должны предоставлять доступ к командной строке.
- Для программ, принимающих права доступа, должна быть задана надежная защита.
- Чрезмерное применение принимаемых прав доступа может снизить производительность системы. Во избежание подобного эффекта ознакомьтесь с блок-схемой проверки прав доступа и предложениями по применению принимаемых прав доступа, приведенными в главе 5 книги *iSeries Security Reference*.

Опции меню SECBATCH:

1 - *передать на выполнение немедленно,* **40** - *поместить в планировщик заданий*

С помощью команды Печатать принимающие объекты (PRTADPOBJ) (опция 21 в меню SECTOOLS) вы можете отслеживать использование в системе принимаемых прав доступа.

В выводе этой команды указываются специальные права доступа, предоставленные заданному пользовательскому профайлу, список программ, принимающих права доступа этого профайла, а также список устройств ASP, применяющих права доступа профайла. После создания базы информации вы можете регулярно печатать только отчеты об изменениях в принятых объектах. В таком отчете будут перечислены программы, принимающие права, и программы, в которые была добавлена такая возможность с момента последнего запроса этого отчета.

Если вам кажется, что принятые права доступа используются в системе не по назначению, вы можете изменить системное значение QAUDLVL, включив в него *PGMADP. Если это значение активно, то система будет создавать запись журнала контроля при каждом запуске или завершении программы, принимающей права доступа. Такая запись содержит имя пользователя, запустившего программу, и имя программы.

Настройка ограничения на применение принятых прав доступа

При запуске программа iSeries может использовать принятые права доступа одним из двух способов:

- Программа может принять права доступа у своего владельца. Владелец указывается в параметре Пользовательский профайл (USRPRF) программы или службы.
- Программа может унаследовать принятые права доступа от предыдущей программы, все еще находящейся в стеке вызовов задания. Программа может унаследовать принятые права доступа от предыдущих программ, даже если она сама не принимает права доступа. Наследование прав доступа от предыдущих программ в стеке вызовов контролируется параметром Применять принятые права доступа (USEADPAUT) программы или службы.

Ниже приведен пример наследования принятых прав доступа от предыдущей программы.

Пусть у пользовательского профайла ICOWNER есть права доступа *CHANGE к файлу ITEM, в то время как общие права доступа к файлу ITEM - *USE. У всех остальных пользовательских профайлов нет явно предоставленных прав доступа к файлу ITEM. Атрибуты трех программ, работающих с файлом ITEM, показаны в Табл. 14:

Таблица 14. Пример использования параметра Применять принятые права доступа (USEADPAUT)

Имя программы	Владелец программы	Значение USRPRF	Значение USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Пример 1 – Использование принятых прав доступа
1. USERA запускает программу PGMA.
2. Программа PGMA пытается открыть файл ITEM для обновления.

Результат: Попытка будет успешной. У USERA есть права доступа *CHANGE к файлу ITEM, принятые программой PGMA от пользователя ICOWNER.

Пример 2 – Использование принятых прав доступа
1. USERA запускает программу PGMA.

2. Программа PGMA вызывает программу PGMB.
3. Программа PGMB пытается открыть файл ITEM для обновления.

Результат: Попытка будет успешной. Хотя программа PGMB не принимает права доступа (параметр USRPRF равен *USER), для нее разрешено наследование принятых прав доступа (параметр USEADPAUT равен *YES). Программа PGMA все еще находится в стеке программ. Таким образом, USERA получает права доступа *CHANGE к файлу ITEM, принятые программой PGMA от пользователя ICOWNER.

Пример 3 – Игнорирование принятых прав доступа
1. USERA запускает программу PGMA.
2. Программа PGMA вызывает программу PGMC.
3. Программа PGMC пытается открыть файл ITEM для обновления.

Результат: Попытка будет неудачной из-за недостаточных прав доступа. Программа PGMC не принимает права доступа. Кроме того, программе PGMC не разрешено наследовать права доступа от предыдущих программ. Хотя программа PGMA все еще находится в стеке задания, ее принятые права доступа не используются.

Настройка запрета на наследование принятых прав доступа новыми программами

Наследование принятых прав доступа новыми программами в стеке позволяет искушенному программисту создать программу ″троянский конь″. Эта программа может использовать предыдущие программы стека задания для получения дополнительных прав доступа, необходимых для несанкционированных действий. Для предотвращения такой ситуации можно запретить пользователям создавать программы, наследующие принятые права доступа у предыдущих программ.

При создании новой программы система автоматически присваивает параметру USEADPAUT значение *YES. Для того чтобы программа не могла наследовать права доступа, укажите в этом параметре значение *NO командой Изменить программу (CHGPGM) или Изменить служебную программу (CHGSRVPGM).

С помощью списка прав доступа и системного значения Применять принятые права доступа (QUSEADPAUT) можно указать, каким пользователям разрешено создавать программы, наследующие принятые права доступа. Система применяет список прав доступа, указанный в системном значении QUSEADPAUT, для определения режима создания новых программ.

Система проверяет указанный список прав доступа при создании пользователем программы или службы. Если у пользователя есть права доступа *USE, параметру USEADPAUT новой программы присваивается значение *YES; если нет, то - значение *NO. Права доступа пользователя к списку прав доступа не могут быть принятыми.

Список прав доступа, указанный в системном значении QUSEADPAUT, определяет также права на изменение параметра USEADPAUT программы или службы командой CHGxxx.

Примечания:

1. Вам не обязательно указывать свой список прав доступа QUESADPAUT. Можно создать список прав доступа с другим именем и указать его в системном значении QUSEADPAUT. В командах из приведенного ниже примера укажите имя своего списка прав доступа.

2. Системное значение QUSEADPAUT не влияет на работу программ, уже установленных в системе. Для того чтобы задать параметр USEADPAUT для существующих программ, вызовите команду CGHPGM или CHGSRVPGM.

Более строгие требования к защите: Для того чтобы большинство пользователей могли создавать программы только с параметром USEADPAUT, равным *NO, выполните следующие действия:

1. Для того чтобы задать общие права доступа к списку прав доступа равными *EXCLUDE, введите следующую команду:

   ```
   CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
      AUT(*EXCLUDE)
   ```

2. Для того чтобы предоставить пользователям права на создание программ, наследующих принятые права доступа, введите следующую команду:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(имя-пользователя)
      AUT(*USE)
   ```

Менее строгие требования к защите: Для того чтобы большинство пользователей могли создавать программы с параметром USEADPAUT, равным *YES, выполните следующие действия:

1. Оставьте общие права доступа к списку прав доступа равными *USE.
2. Для того чтобы запретить пользователям создание программ, наследующих принятые права доступа, введите следующую команду:

   ```
   ADDAUTLE AUTL(QUSEADPAUT)
      USER(имя-пользователя) AUT(*EXCLUDE)
   ```

Контроль за применением программ триггера

В DB2 UDB предусмотрена возможность связывать программы триггера с файлами баз данных. Такая функция применяется обычно при создании многофункциональных диспетчеров баз данных.

При связывании программы триггера с файлом базы данных вы задаете условия запуска программы триггера. Например, вы можете настроить файл заказа покупателя так, чтобы он запускал программу триггера при добавлении в него новой записи. Можно задать запуск программы триггера при превышении просроченным платежом заказчика уровня кредита, чтобы эта программа отправляла заказчику сообщение с предупреждением и информировала менеджера по кредитам.

Программы триггера представляют собой эффективный способ вызова функций приложений и управления информацией. Они же предоставляют возможность злоумышленнику создать “Троянского коня” в вашей системе. Вредоносная программа, незаметно поселившись в вашей системе, может дожидаться специального события в файле базы данных, который послужит причиной ее запуска.

Примечание: Исторически, Троянский конь - это подарок греков жителям Трои в виде большого деревянного коня, внутри которого сидели греческие воины. После того как конь въехал за пределы крепости Трои, воины выскочили из коня и захватили Трою. В компьютерной терминологии Троянским конем часто называется программа, содержащая разрушительные для системы функции.

Опции меню SECBATCH:
27 - *передать на выполнение немедленно*, **66** - *поместить в планировщик заданий*

Система поставляется с запрещенной функцией добавления программы триггера к файлу базы данных. Если управление правами доступа к объектам выполняется грамотно, то у обычных пользователей нет прав на связывание программы триггера с файлом базы данных. (В приложении D книги *iSeries Security Reference* указано, какие права доступа необходимы, а также перечислены все команды, в том числе и Добавить триггер физического файла (ADDPFTRG)).

С помощью команды Печатать программы триггера (PRTTRGPGM) вы можете напечатать список всех программ триггера из указанной библиотеки или из всех библиотек.

Начальный отчет можно принять за основу для учета всех программ триггера, существующих в системе. В дальнейшем можно печатать только отчет об изменениях, в котором будут перечисляться программы триггера, добавленные в систему.

При учете программ триггера следует обратить внимание на следующее:

- Кто создал программу-триггера? Вы можете определить это с помощью команды Показать описание объекта (DSPOBJD).
- Что выполняет данная программа? Получите эти сведения у автора программы или просмотрите код программы. Например, не выполняет ли эта программа идентификацию пользователя? Возможно, программа триггера ожидает входа в систему конкретного пользователя (QSECOFR), чтобы получить через него доступ к ресурсам системы.

После создания базы информации вы можете регулярно печатать только отчеты об изменениях для отслеживания программ триггера, добавляемых в систему.

Обнаружение скрытых программ

Программы триггера - это не единственный способ проникновения в систему ″троянского коня″. Они служат всего лишь примером **программ выхода**. Если в системе происходит какое-либо событие (в случае программы триггера таким событием может быть обновление файла), то запускается программа выхода, связанная с этим событием.

В Табл. 15 на стр. 82 приводятся другие примеры программ выхода, которые могут существовать в вашей системе. Для проверки кода этих программ, а также их назначения, вы можете воспользоваться теми же способами, что и для проверки программ триггера.

Примечание: В Табл. 15 на стр. 82 перечислены не все возможные программы выхода.

.

Таблица 15. Системные программы выхода

Имя программы	**Когда запускается**
Имя, указанное пользователем в сетевом атрибуте DDMACC.	При попытке пользователя открыть файл DDM в системе или установить соединение DRDA.
Имя, указанное пользователем в сетевом атрибуте PCSACC.	При попытке пользователя с помощью Original Clients обратиться к функциям Client Access для доступа к объектам системы.
Имя, указанное пользователем в системном значении QPWDVLDPGM	При вызове пользователем функции Изменить пароль.
Имя, указанное пользователем в системном значении QRMTSIGN.	При попытке удаленного пользователя войти в систему в интерактивном режиме.
QSYS/QEZUSRCLNP	При вызове функции автоматической очистки.
Имя, указанное пользователем в параметре EXITPGM команды CHGBCKUP.	При вызове функции резервного копирования Операционной поддержки.
Имя, указанное пользователем в команде CRTPRDLOD.	До и после сохранения, восстановления или удаления продукта, созданного с помощью этой команды.
Имя, указанное пользователем в параметре DFTPGM команды CHGMSGD.	Если для сообщения задана программа по умолчанию, то она будет выполняться системой при выдаче сообщения. Поскольку обычно в системе существует много описаний сообщений, работу программ по умолчанию отслеживать достаточно сложно. Для того чтобы запретить пользователям с общими правами доступа добавление программ по умолчанию для сообщений, установите в качестве общих прав доступа к файлам сообщений (объектам *MSGF) значение *USE.
Имя, указанное пользователем в параметре FKEYPGM команды STREML3270.	При нажатии пользователем функциональной клавиши во время сеанса эмуляции устройства 3270. По завершении программы выхода система передает управление сеансу эмуляции устройства 3270.
Имя, указанное пользователем в параметре EXITPGM команды монитора сбора статистики.	Программа запускается для обработки данных, собранных с помощью следующих команд: STRPFRMON, ENDPFRMON, ADDPFRCOL и CHGPFRCOL. Она вызывается после завершения сбора данных.
Имя, указанное пользователем в параметре EXITPGM команды RCVJRNE.	При чтении записи журнала или группы записей журнала из заданного журнала или получателя журнала.
Имя, указанное пользователем в API QTNADDCR.	Во время операции COMMIT или ROLLBACK.
Имя, указанное пользователем в API QHFRGFS.	При вызове функций файловой системы
Имя, указанное пользователем в параметре SEPPGM описания принтера.	Программа определяет, что нужно печатать на разделительной странице, которая выдается до или после печати буферного файла или задания печати.
QGPL/QUSCLSXT	Программа вызывается при закрытии файла базы данных для сбора информации об использовании файла.
Имя, указанное в параметре FMTSLR логического файла.	При занесении записи в файл базы данных, если имя формата записи не задано в программе на языке высокого уровня. Программа получает эту запись в качестве входного параметра, определяет формат записи и возвращает его в базу данных.
Имя, указанное пользователем в системном значении QATNPGM, в параметре ATNPGM пользовательского профайла или в параметре PGM команды SETATNPGM.	При нажатии пользователем клавиши Attention.
Имя, указанное пользователем в параметре EXITPGM команды TRCJOB.	Перед запуском процедуры Трассировка задания.

Убедитесь, что значение по умолчанию для параметра, задающего программу выхода, не изменено ни в одной команде, поддерживающей этот параметр. Кроме того, вы должны установить такие общие права доступа к этим командам, которые не позволяют изменять значения по умолчанию параметров команды. Для вызова команды CHGCMDDFT нужны права доступа *OBJMGT. Для запуска других команд эти права доступа не нужны, поэтому предоставлять их не нужно.

Просмотр зарегистрированных программ выхода

Системная функция регистрации предназначена для регистрации программ выхода, которые должны запускаться при возникновении определенных событий. Для того чтобы просмотреть список программ выхода, зарегистрированных в системе, введите команду `WRKREGINF OUTPUT(*PRINT)`. На рис. 8 показан пример вывода этой команды:

```
                Работа с регистрационной информацией
Точка выхода . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Формат точки выхода. . . . . . . . . . :   NJEO0100
Точка выхода зарегистрирована  . . . . :   *YES
Разрешить отмену регистрации . . . . . :   *YES
Максимальное число программ выхода . . :   *NOMAX
Текущее число программ выхода  . . . . :   0
Предв. обработка при добавлении. . . . :   *NONE
  Библиотека . . . . . . . . . . . . . :
  Формат . . . . . . . . . . . . . . . :
Предв. обработка при удалении. . . . . :   *NONE
  Библиотека . . . . . . . . . . . . . :
  Формат . . . . . . . . . . . . . . . :
Предв. обработка при просмотре . . . . :   *NONE
  Библиотека . . . . . . . . . . . . . :
```

Рисунок 8. Пример отчета, выдаваемого командой Работа с регистрационной информацией

Для каждой точки выхода системы в отчете будет показано, зарегистрированы ли программы выхода. Если да, вы можете просмотреть информацию об этих программах, выбрав опцию 8 (Показать программы) меню WRKREGINF:

```
                    Работа с регистрационной информацией

Введите опции, нажмите Enter.
5=Показать точку выхода   8=Работа с программами выхода

                          Формат
     Точка                точки
Опц  выхода               выхода    Зарегистр.  Описание
     QIBM_QGW_NJEOUTBOUND NJEO0100     *YES     Запись о сетевом задании
8    QIBM_QHQ_DTAQ        DTAQ0100     *YES     Сервер очереди исходных данных
     QIBM_QLZP_LICENSE    LICM0100     *YES     Сервер управления лицензиями
     QIBM_QMF_MESSAGE     MESS0100     *YES     Сервер исходных сообщений
     QIBM_QNPS_ENTRY      ENTR0100     *YES     Сервер сетевой печати - ввод
     QIBM_QNPS_SPLF       SPLF0100     *YES     Сервер сетевой печати - буфер
     QIBM_QNS_CRADDACT    ADDA0100     *YES     Процедура Добавить описание CRQ
     QIBM_QNS_CRCHGACT    CHGA0100     *YES     Процедура Изменить описание CRQ
```

Для проверки этих программ выхода воспользуйтесь тем же способом, что и для проверки других программ выхода и программ триггера.

Просмотр запланированных программ

В iSeries существуют различные средства для планирования запуска задач, например, планировщик заданий. Как правило, применение этих средств не представляет угрозу безопасности системы, так как для планирования запуска задания необходимы те же права доступа, что и для запуска этого задания в пакетном режиме.

Тем не менее, рекомендуется периодически проверять, запуск каких заданий запланирован на будущее. Так, перед увольнением пользователь может запланировать запуск задания, которое приведет к сбою системы.

Ограничение доступа к командам сохранения и восстановления

Большинству пользователей не требуется сохранять и восстанавливать объекты в системе. Команды сохранения предназначены для копирования важной информации на носители данных или в другую систему. Большая часть команд сохранения поддерживает копирование в файл сохранения, который затем можно передать в другую систему (с помощью команды SNDNETF). Для выполнения таких команд права доступа к носителю или устройству сохранения/восстановления не требуются.

С помощью команд восстановления пользователь потенциально может восстановить в системе объекты, в том числе программы, команды и файлы, доступ к которым ему запрещен. Файлы сохранения позволяют восстановить информацию без помощи носителя или устройства сохранения/восстановления. Такие файлы сохранения могут быть переданы из другой системы с помощью команды SNDNETF или по FTP.

Ниже приведены рекомендации по ограничению доступа к командам сохранения и восстановления:

- Предоставьте права доступа *SAVSYS лишь тем пользователям, которым они действительно необходимы. Специальные права доступа *SAVSYS позволяют пользователю сохранять и восстанавливать объекты, даже если у этого пользователя нет необходимых прав доступа к этим объектам.
- Управление доступом к устройствам сохранения и восстановления.
- Ограничьте права доступа к командам сохранения и восстановления. В версиях V4R3 и V3R7 лицензионной программы OS/400 общие права доступа к команде RSTxxx равны *EXCLUDE, а общие права доступа к команде SAVxxx равны *USE. Рекомендуется установить для команд SAVxxx общие права доступа *EXCLUDE. Соблюдайте осторожность, предоставляя пользователям права на выполнение команд RSTxxx.
- Для ограничения прав на восстановление программы режима системы, программы, принимающие права доступа, объекты с ошибками, обнаруженными при проверке
- Системное значение QVFYOBJRST предназначено для управления восстановлением объектов с цифровыми подписями в системе.
- С помощью системного значения QFRCCVNRST можно указать, следует ли заново создавать объекты во время их восстановления в системе.
- Для отслеживания операций восстановления используйте функцию контроля за действиями в системе. Укажите в системном значении QAUDLVL параметр *SAVRST и периодически печатайте контрольные записи, создаваемые операциями восстановления. (Дополнительная информация о работе с контрольными записями приведена в главе 9 и приложении F книги *iSeries Security Reference*.)

Поиск пользовательских объектов в защищенных библиотеках

С каждым заданием сервера iSeries связан список библиотек. В этом списке определена последовательность поиска системой объекта в том случае, если не указана его библиотека. Например, если вы вызвали программу, не указав, в какой библиотеке она находится, система просмотрит заданный список библиотек и запустит первую встреченную копию этой программы.

В книге *iSeries Security Reference* приведена дополнительная информация о рисках применения списков библиотек и о вызове программ без указания имени библиотеки (такой вызов называется **неточным вызовом**). В ней также приведены предложения по управлению содержимым списков библиотек и информация об изменении списков.

Для правильной работы вашей системы в список библиотек для любого задания должны быть включены некоторые системные библиотеки, такие как QSYS и QGPL. Контроль за добавлением программ в эти библиотеки должен осуществляться путем управления доступом к объектам. Таким образом вы сможете предотвратить добавление в одну из таких библиотек посторонней программы с таким же именем, что и у программы в библиотеке, идущей в списке после этих библиотек.

Рекомендуется также контролировать работу пользователей с правами доступа к команде CHGSYSLIBL и отслеживать записи SV в журнале контроля за действиями. Некий злоумышленник может поместить какую-либо библиотеку в список библиотек перед QSYS, в результате чего при вызове другими пользователями команд, поставляемых фирмой IBM, будут запускаться другие команды с такими же именами.

Опции меню SECBATCH:

28 - *передать на выполнение немедленно,* **67** - *поместить в планировщик заданий*

С помощью команды Печатать пользовательские объекты (PRTUSROBJ) можно просмотреть список пользовательских объектов (объектов, не поставляемых фирмой IBM), расположенных в указанной библиотеке. Проанализировав полученный список программ, вы сможете определить, кто их создал и какие функции они выполняют.

Пользовательские объекты, не являющиеся программами, также могут представлять собой опасность для системы, если они находятся в системных библиотеках. Например, если программа записывает конфиденциальные данные в файл с неполным именем, то злоумышленник может поместить в системную библиотеку ложную версию этого файла, которая и будет применена программой.

Глава 10. Предотвращение и выявление постороннего вмешательства

В этом разделе собраны советы по выявлению слабых мест в защите и предотвращению постороннего вмешательства в работу системы.

Физическая защита

С одной стороны, системный блок - это имущество вашей фирмы, а с другой стороны - устройство, которое обеспечивает работу системы. Внутри системного блока находится множество мелких, но важных деталей. Он должен быть размещен таким образом, чтобы никто не мог разобрать системный блок и достать важные компоненты.

На системном блоке есть панель управления, которая позволяет выполнять основные функции, не пользуясь рабочей станцией. Например, с помощью панели управления можно выполнить следующие действия:

- Выключить систему.
- Включить систему.
- Загрузить операционную систему.
- Выполнить служебные функции.

Выполнение любой из этих функций потенциально может повредить информацию и параметры пользователей системы. Кроме того, эти функции представляют потенциальную угрозу для безопасности системы. Для ограничения доступа к перечисленным функциям предназначен замок с ключом. Для того чтобы заблокировать панель управления, поверните ключ в положение Secure. После этого вытащите и спрячьте ключ.

Примечания:

1. Если вам необходимо выполнять удаленную IPL или удаленную диагностику системы, рекомендуется установить ключ в другое положение. Дополнительная информация об установке переключателя приведена в разделе Введение в iSeries Information Center (подробная информация приведена в разделе “Необходимая и полезная информация” на стр. xii).
2. Замок с ключом не входит в стандартную комплектацию некоторых моделей системы.

Отслеживание действий над пользовательскими профайлами

Каждый пользователь входит в систему и работает в ней под управлением некоторого пользовательского профайла. Параметры этого профайла определяют среду работы и характеристики защиты для данного пользователя. Администратор системы должен отслеживать и контролировать изменения, вносимые в пользовательские профайлы системы.

Контроль за защитой можно настроить таким образом, чтобы информация об изменениях в пользовательских профайлах регистрировалась. Эту информацию можно затем напечатать с помощью команды DSPAUDJRNE.

Вы можете создать программы выхода, которые будут отслеживать запрошенные действия над пользовательскими профайлами. В Табл. 16 на стр. 88 представлены

точки выхода, доступные для команд работы с пользовательскими профайлами.

Таблица 16. Точки выхода команд работы с пользовательскими профайлами

Команда	Имя точки выхода
Создать пользовательский профайл (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Изменить пользовательский профайл (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
Удалить пользовательский профайл (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Восстановить пользовательский профайл (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

С помощью программы выхода можно, например, отслеживать изменения, которые могут позволить пользователю запускать неразрешенную версию программы или назначить другое описание задания или новую текущую библиотеку. Программу выхода можно настроить таким образом, чтобы она передавала уведомление в очередь сообщений или выполняла какое-либо действие (например, изменение или отключение пользовательского профайла) в зависимости от полученной информации.

Подробная информация о применении программ выхода к пользовательским профайлам приведена в книге *iSeries Security Reference*.

Создание подписей объектов

Все меры по защите системы бесполезны, если их можно обойти, разместив в системе посторонние данные. На сервере iSeries предусмотрено большое число встроенных функций, с помощью которых можно предотвратить загрузку в систему постороннего программного обеспечения и обнаружить уже загруженные посторонние программы. В выпуске V5R1 эти функции были дополнены возможностью создания электронных подписей объектов.

Подписи объектов в iSeries - это реализация приема шифрования, называемого ″цифровыми подписями″. Идея очень проста: поставщик программного обеспечения ″подписывает″ свои продукты. Эту подпись нельзя рассматривать как гарантию выполнения той или иной функции. Подпись подтверждает, что программное обеспечение поставлено указанным производителем и не изменялось с момента его создания и подписания. Гарантия подлинности приобретает особое значение, когда программное обеспечение передается по сети Internet или хранится на носителях, доступных другим лицам.

Применение цифровых подписей ужесточает контроль за программным обеспечением, загружаемым в систему, и позволяет быстрее обнаруживать изменения, внесенные в уже загруженное программное обеспечение. Новое системное значение Проверить восстановление объекта (QVFYOBJRST) позволяет задавать ограничивающую стратегию, разрешающую загружать программное обеспечение только при условии, что оно подписано известными фирмами-производителями. Вы можете выбрать и другую, более мягкую стратегию, при которой вы будете только проверять подписи, если они есть.

Все программное обеспечение OS/400, а также лицензионные программы и дополнительные компоненты для iSeries подписаны уполномоченной организацией. Эти подписи помогают защитить целостность системы; они проверяются при установке в системе исправлений с целью убедиться, что исправление поступило от уполномоченной организации и не было изменено при передаче. Можно также

проверять цифровые подписи программного обеспечения после его установки в системе. Команда CHKOBJITG (Проверить целостность объектов) теперь позволяет проверять также и цифровые подписи объектов. Кроме того, у программы Диспетчер цифровых сертификатов появились новые панели, которые позволяют проверять подписи объектов, включая объекты операционной системы.

Цифровые подписи позволяют защитить целостность не только операционной системы, но и важного программного обеспечения. Вы можете приобрести программное обеспечение, подписанное производителем, или подписать купленное или созданное вами программное обеспечение. Впоследствии в рамках стратегии защиты вы можете периодически проверять подписи этих объектов с помощью команды CHKOBJITG или Диспетчера цифровых сертификатов. Кроме того, в своей стратегии защиты вы можете предусмотреть требование, чтобы все программное обеспечение, которое восстанавливается в системе, было подписано вами или надежным источником. Однако поскольку большая часть программного обеспечения других фирм, предназначенного для iSeries, поставляется без цифровой подписи, такая стратегия может оказаться слишком неудобной. В целом, поддержка цифровых подписей значительно расширяет ваши возможности по выбору стратегии защиты целостности программного обеспечения.

Цифровые подписи для защиты программного обеспечения - это лишь один из способов применения цифровых сертификатов. Дополнительная информация по работе с цифровыми сертификатами приведена в разделе ″Управление цифровыми сертификатами″ Information Center (подробную информацию см. в разделе “Необходимая и полезная информация” на стр. xii).

Просмотр описаний подсистем

При запуске подсистемы на сервере iSeries система создает рабочую среду, позволяющую войти в систему и работать с ней. Вид этой среды определяется описанием подсистемы. Описания подсистем предоставляют потенциальную возможность несанкционированного доступа к системе. Например, с помощью описания подсистемы злоумышленник может настроить автоматический запуск программы или разрешить вход в систему без проверки пользовательского профайла.

При выполнении команды Аннулировать общие права доступа (RVKPUBAUT) общие права доступа к командам, предназначенным для работы с описанием подсистемы, устанавливаются равными *EXCLUDE. При этом пользователям, у которых нет необходимых прав доступа (или специальных прав доступа *ALLOBJ) запрещается изменять или создавать описания подсистем.

В данном разделе даются рекомендации по контролю за существующими в вашей системе описаниями подсистем. Для получения списка описаний всех подсистем введите команду WRKSBSD (Работа с описаниями подсистем). Если вы укажете опцию 5 (Показать) напротив описания подсистемы, то появится меню с выбранным описанием подсистемы. В этом меню перечислены компоненты описания подсистемы.

Для того чтобы получить подробную информацию о компоненте, выберите соответствующую опцию. Для изменения первых двух компонентов вызовите команду CHGSBSD (Изменить описание подсистемы). Для изменения информации, содержащейся в остальных пунктах, используйте команды добавления, удаления или изменения для соответствующего типа записи. Например, для изменения записи рабочей станции введите команду CHGWSE (Изменить запись рабочей станции).

Дополнительная информация о работе с описаниями подсистем приведена в книге *Work Management*. Там же содержится список стандартных значений для описаний подсистем, поставляемых фирмой IBM.

Записи автоматических заданий

Запись автоматического задания содержит имя описания задания. Описание задания может содержать запрос (RQSDTA) на запуск программы или выполнение команды. Например, в качестве RQSDTA может быть указано `CALL LIB1/PROGRAM1`. В этом случае при запуске подсистемы будет выполняться программа PROGRAM1 из библиотеки LIB1.

Просмотрите все записи автоматических заданий и связанные с ними описания. Убедитесь в том, что вы знаете, какие действия выполняет каждая программа, автоматически запускаемая при запуске подсистемы.

Имена и типы рабочих станций

При запуске подсистемы ей выделяются все свободные рабочие станции, указанные (явным образом или в виде шаблонов) в записях имен и типов рабочих станций. При входе пользователя в систему он попадает в ту подсистему, которой выделена соответствующая рабочая станция.

В записи рабочей станции указывается описание задания, которое должно применяться при запуске задания на данной рабочей станции. Описание задания может содержать запрос на запуск программы или команды. Например, в параметре RQSDTA может быть указано `CALL LIB1/PROGRAM1`. В этом случае при входе пользователя на рабочую станцию данной подсистемы будет запускаться программа PROGRAM1 из библиотеки LIB1.

Просмотрите записи рабочих станций и связанные с ними описания заданий. Убедитесь, что в запросы на запуск программ не внесено изменений, о которых вы не знаете.

В записи рабочей станции также может быть задан пользовательский профайл, применяемый по умолчанию. В подсистемах с некоторыми конфигурациями это позволяет войти в систему, просто нажав клавишу Enter. Если уровень защиты в системе (системное значение QSECURITY) меньше 40, то вы должны просмотреть записи рабочих станций и проверить, не заданы ли в них профайлы по умолчанию.

Записи очередей заданий

При запуске подсистемы ей выделяются все незаблокированные очереди заданий, указанные в описании подсистемы. Записи очередей заданий сами по себе не представляют никакой угрозы безопасности. Однако с их помощью можно запускать задания в не предназначенной для этого среде и, тем самым, оказывать влияние на производительность системы.

Вы должны периодически просматривать записи очередей заданий и проверять, что пакетные задания выполняются в соответствующей среде.

Записи о выполнении

Запись о выполнении определяет, что делает задание при поступлении в подсистему. Записи о выполнении применяются подсистемой для всех типов заданий: пакетных, интерактивных и заданий средств связи. Запись о выполнении задает:

- класс задания. Как и записи очередей заданий, класс, связанный с заданием, влияет на скорость выполнения задания, но не представляет никакой потенциальной угрозы для безопасности системы.
- программу, которая начинает работать при запуске задания. Просмотрите записи о выполнении и убедитесь, что в них не заданы программы, запуск которых нежелателен.

Записи соединений и имена удаленных расположений

При получении удаленного задания система определяет, каким образом будет выполняться это задание, на основании записей соединений и записей имен удаленных расположений из описания активной подсистемы. В этих записях необходимо проверять следующее:

- Задания из удаленных систем могут запускаться во всех подсистемах. Если подсистема, в которой должно было выполняться удаленное задание, неактивна, то это задание может найти необходимую запись в описании другой подсистемы. Поэтому вы должны проверить все записи в описаниях всех подсистем.
- В записи соединения задается описание задания. Описание задания может содержать запрос на запуск программы или команды. Просмотрите все записи соединений и связанные с ними описания заданий и убедитесь, что при запуске заданий не запускаются нежелательные программы и команды.
- Запись соединения также содержит имя пользовательского профайла по умолчанию, который в некоторых случаях применяется системой. Убедитесь, что вам ясна роль профайла по умолчанию. Если в вашей системе есть профайлы по умолчанию, предоставьте им лишь минимальные права доступа. Информация о пользовательских профайлах по умолчанию приведена в разделе Глава 12, “Защита соединений APPC”.

  Для того чтобы узнать имена профайлов по умолчанию, заданные в записях соединений, введите команду PRTSBSDAUT (Печать описания подсистемы).

Записи предварительных заданий

С помощью записей предварительных заданий можно подготовить систему к запуску некоторых заданий, сократив тем самым время их выполнения. Предварительные задания могут запускаться как при запуске подсистемы, так и в любое другое время. В записи предварительного задания указываются следующие параметры:

- программа, которая будет запускаться

  пользовательский профайл по умолчанию

  описание задания

Изменение любого из этих параметров может привести к нарушению защиты системы. Вы должны убедиться, что предварительные задания выполняют только допустимые действия, не нарушающие защиту.

Задания и их описания

В описании задания содержатся данные запроса и данные о выполнении, в которых может быть задана программа, запускаемая при использовании данного описания задания. Если параметр данных запроса в описании задания содержит имя программы, то система запустит эту программу. Если в описании задания заданы данные о выполнении, система запустит программу, заданную в соответствующей записи о выполнении.

Описания заданий используются системой и для интерактивных, и для пакетных заданий. Для интерактивных заданий описание задания указывается в записи рабочей станции. Обычно для записи рабочей станции задается значение *USRPRF, поэтому система использует описание задания, которое указано в пользовательском профайле. Для пакетных заданий описание задания указывается при передаче задания на выполнение.

Вы должны периодически просматривать описания заданий и проверять, не содержат ли они запросов на запуск запрещенных программ. С помощью прав доступа к объектам запретите изменять описания заданий. Для запуска задания с указанным описанием достаточно прав доступа *USE. Не предоставляйте обычным пользователям права доступа *CHANGE к описаниям заданий.

Опции меню SECBATCH:
15 - *немедленно передать на выполнение;* **54** - *запланировать запуск*

В описании задания может быть задан пользовательский профайл, под управлением которого должно выполняться задание. Если уровень защиты не ниже 40, у вас должны быть права доступа *USE к описанию задания и к указанному в этом описании пользовательскому профайлу. Если уровень защиты ниже 40, то нужны лишь права доступа *USE к описанию задания.

Для того чтобы просмотреть список описаний заданий, в которых заданы пользовательские профайлы, и для которых установлены общие права доступа *USE, вызовите команду PRTJOBDAUT (Печать прав доступа к описанию задания).

В отчете показано, какие специальные права доступа предоставлены пользовательскому профайлу, указанному в описании задания. Кроме того, в отчете перечислены специальные права доступа всех групп, к которым относится данный пользовательский профайл. Для просмотра частных прав доступа пользовательского профайла введите команду:

```
DSPUSRPRF USRPRF(имя-профайла) TYPE(*OBJAUT)
```

Описание задания содержит список библиотек, используемых при выполнении задания. Если кто-то изменит список библиотек пользователя, то этот пользователь сможет запускать запрещенную версию программы из другой библиотеки. По этой причине вы должны периодически проверять списки библиотек, указанные в описаниях заданий.

И, наконец, вы должны проверять, не изменены ли значения по умолчанию для команд SBMJOB (Передать задание на выполнение) и CRTUSRPRF (Создать пользовательский профайл), определяющие описания заданий.

Архитектурные имена программ транзакций

Некоторые запросы на соединение передают в систему сигнал определенного типа. Этот запрос называется **архитектурное имя программы транзакций (TPN)**, поскольку имя программы транзакций представляет собой компонент архитектуры APPC для системы. Примером архитектурного TPN может служить запрос на удаленный вход в систему дисплейной станции. Архитектурные TPN представляют собой обычный способ функционирования соединений и не всегда представляют угрозу безопасности системы. Однако они предоставляют возможность для несанкционированного доступа в систему.

В некоторых запросах TPN имя профайла не передается. Если такой запрос связывается с записью соединения, в которой указан пользователь по умолчанию *SYS, то система может начать обработку запроса. Однако профайлу *SYS разрешено выполнять только системные функции, но не пользовательские приложения.

Если вы не хотите, чтобы архитектурные TPN выполнялись с профайлом по умолчанию, то укажите в записях соединений вместо пользователя по умолчанию *SYS значение *NONE. Список архитектурных TPN и связанных с ними профайлов приведен в “Запросы архитектурного TPN”.

Если вы хотите, чтобы запрос TPN не выполнялся в системе, выполните следующие действия:

1. Создайте программу на CL, в которую будут передаваться несколько параметров. Эта программа, не выполняющая никаких функций, должна содержать только объявления (DCL) параметров.
2. Добавьте запись о выполнении для данного TPN в описания всех подсистем, содержащие записи соединений или записи имен удаленных расположений. В записи о выполнении должны быть заданы следующие параметры:
   - В качестве *Значение сравнения* (CMPVAL) должно быть задано имя программы для TPN (см. Запросы архитектурного TPN) с начальной позицией 37.
   - В качестве *Вызываемой программы* (PGM) должно быть задано имя программы, созданной на шаге 1. Таким образом запросу TPN будет запрещено применять другие записи о выполнении, например, *ANY.

Подсистема QCMN уже содержит записи о выполнении для некоторых TPN. Они были добавлены для оптимизации работы системы.

Запросы архитектурного TPN

Таблица 17. Программы и пользователи запросов TPN

Запрос TPN	Программа	Пользовательский профайл	Описание
X'30F0F8F1'	AMQCRC6A	*NONE	Управление очередями сообщений
X'06F3F0F1'	QACSOTP	QUSER	Программа транзакции входа в APPC
X'30F0F2D1'	QANRTP	QADSM	Настройка APPC ADSM/400
X'30F0F1F9'	QCNPCSUP	*NONE	Папки AS/400
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	Удаленный SQL–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	Получатель DSNX–PC
X'30F0F1F3'	QDXPSEND	QUSER	Отправитель DSNX–PC
X'30F0F2C4'	QEVYMAIN	QUSER	Сервер ENVY**/400
X'30F0F6F0'	QHQTRGT	*NONE	Очередь данных PC
X'30F0F8F0'	QLZPSERV	*NONE	Администратор лицензий Client Access
X'30F0F1F7'	QMFRCVR	*NONE	Получатель сообщений PC
X'30F0F1F8'	QMFSNDR	*NONE	Отправитель сообщений PC
X'30F0F6F6'	QND5MAIN	QUSER	Контроллер рабочей станции APPN 5394
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA

Таблица 17. Программы и пользователи запросов TPN (продолжение)

Запрос TPN	Программа	Пользовательский профайл	Описание
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Утилиты управления системой
X'30F0F2C1'	QNPSERVR	*NONE	Сетевой сервер печати PWS-I
X'30F0F7F9'	QOCEVOKE	*NONE	Межсистемный календарь
X'30F0F6F1'	QOKCSUP	QDOC	Создание теневых каталогов
X'20F0F0F7'	QOQSESRV	QUSER	DIA версии 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA версии 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA версии 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA версии 1
X'30F0F0F5'	QPAPAST2	QUSER	Удаленный вход в систему S/36—S/38
X'30F0F0F9'	QPAPAST2	QUSER	Удаленное подключение к принтеру
X'30F0F4F6'	QPWFSTP0	*NONE	Папки AS/400 типа 2
X'30F0F2C8'	QPWFSTP1	*NONE	Файловый сервер Client Access
X'30F0F2C9'	QPWFSTP2	*NONE	Файловый сервер Windows** Client Access
X'30F0F6F9'	QRQSRVX	*NONE	Удаленный объединенный сервер SQL
X'30F0F6F5'	QRQSRV0	*NONE	Удаленный SQL без фиксации
X'30F0F6F4'	QRQSRV1	*NONE	Удаленный SQL без фиксации
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	Получатель FS2 SNADS
X'21F0F0F7'	QS2STSND	QGATE	Отправитель FS2 SNADS
X'30F0F1F6'	QTFDWNLD	*NONE	Функция обмена с PC
X'30F0F2F4'	QTIHNPCS	QUSER	Функция TIE
X'30F0F1F5'	QVPPRINT	*NONE	Виртуальная печать для PC
X'30F0F2D3'	QWGMTP	QWGM	Сервер Ultimedia Mail/400
X'30F0F8F3'	QZDAINIT	QUSER	Сервер данных PWS-I
X'21F0F0F2'	QZDRCVR	QSNADS	Получатель SNADS
X'21F0F0F1'	QZDSTSND	QSNADS	Отправитель SNADS
X'30F0F2C5'	QZHQTRG	*NONE	Сервер данных PWS-I
X'30F0F2C6'	QZRCSRVR	*NONE	Сервер удаленных команд PWS-I
X'30F0F2C7'	QZSCSRVR	*NONE	Центральный сервер PWS-I

Способы контроля за событиями, влияющими на защиту

Защиту системы нельзя настроить раз и навсегда. Вы должны постоянно следить за изменениями в системе и ошибками защиты, а при необходимости - вносить изменения в параметры защиты.

Для отслеживания изменений, влияющих на защиту системы, служат отчеты о защите. Кроме того, для обнаружения ошибок в схеме защиты защиты и предотвращения возможных попыток несанкционированного доступа вы можете использовать другие системные функции:

- Функция контроля за действиями предоставляет возможность отслеживать различные типы событий, происходящих в системе, которые оказывают влияние на защиту. Например, вы можете настроить систему таким образом, чтобы в протокол заносилась контрольная запись каждый раз при открытии определенного файла базы данных для обновления. Вы можете отслеживать все изменения системных значений, а также все действия, выполняемые при восстановлении объектов пользователями.

  Полная информация о функции контроля за действиями приведена в Главе 9 книги *iSeries Security Reference*. Для настройки функции контроля за действиями предназначена команда CHGSECAUD (Изменить контроль за действиями). Кроме того, с помощью команды DSPAUDJRNE (Показать записи журнала контроля) можно напечатать выбранную информацию из журнала контроля за действиями.
- Для сообщений о критических ситуациях вы можете создать очередь сообщений QSYSMSG. В течение рабочего дня многочисленные сообщения разной степени важности направляются в очередь сообщений QSYSOPR. Из-за большого количества сообщений в очереди QSYSOPR можно не заметить сообщения, связанные с защитой.

  Однако, если создать в системе очередь сообщений QSYSMSG в библиотеке QSYS, то система автоматически будет направлять определенные сообщения о критических ситуациях не в QSYSOPR, а в очередь сообщений QSYSMSG.

  Вы можете либо создать программу для контроля за очередью сообщений QSYSMSG, либо настроить очередь таким образом, чтобы сообщения доставлялись вам или другому уполномоченному пользователю в режиме прерывания.

Часть 3. Приложения и сетевые соединения

Глава 11. Защита файлов с помощью Интегрированной файловой системы

Интегрированная файловая система предоставляет несколько способов хранения и просмотра информации на сервере iSeries. Она входит в состав операционной системы OS/400 и отвечает за операции потокового ввода и вывода. По способу управления памятью эта файловая система схожа (и совместима) с операционными системами класса UNIX и операционными системами персональных компьютеров.

С появлением интегрированной файловой системы все объекты можно рассматривать как элементы иерархической структуры каталогов. В большинстве случаев используется то представление объектов, которое наиболее естественно для конкретной файловой системы. Например, стандартные объекты iSeries хранятся в файловой системе QSYS.LIB. Обычно пользователи считают эти объекты элементами библиотеки. Объекты файловой системы QDLS обычно считаются документами, хранящимися в папках. Корневая файловая система (/), а также QOpenSys и пользовательские файловые системы представляют собой иерархическую (многоуровневую) структуру каталогов.

Администратор защиты должен четко представлять следующее:

- Какие файловые системы применяются в системе
- Особенности каждой файловой системы

В следующих разделах приведены некоторые основные сведения о защите при работе с интегрированными файловыми системами.

Защита в Интегрированной файловой системе

Корневая файловая система сервера iSeries играет роль базы для всех прочих файловых систем. Она расположена на самом высоком уровне и содержит все объекты системы. Другие файловые системы сервера iSeries в зависимости от своего назначения предоставляют различные функции для управления объектами и интеграции с другими файловыми системами. Например, файловая система QOPT (оптическая файловая система) позволяет приложениям и серверам iSeries (в том числе файловому серверу iSeries Access для Windows) обращаться к дисководу CD-ROM сервера iSeries. Аналогично, файловая система QFileSvr.400 предоставляет приложениям доступ к данным интегрированной файловой системы, расположенной на удаленном сервере iSeries. Файловый сервер QLANSrv служит для обращения к файлам, хранящимся на Integrated xSeries Server для iSeries или других серверах, подключенных к сети.

Схема защиты отдельной файловой системы зависит от хранящихся в ней данных. Например, файловая система QOPT не поддерживает защиту на уровне объектов, так как не существует технологии записи информации о правах доступа на компакт-диск. За управление доступом к объектам файловой системы QFileSvr.400 отвечает удаленная система (та система, в которой файлы физически расположены). В то же время, за управление доступом к объектам файловых систем, аналогичных QLANSrv, отвечает Integrated xSeries Server для iSeries. Несмотря на все различия в моделях защиты, многие файловые системы поддерживают команды управления доступом интегрированной файловой системы, такие как Изменить права доступа (CHGAUT) и Изменить владельца (CHGOWN).

Ниже приведены некоторые замечания о ″подводных камнях″, с которыми вы можете встретиться при настройке защиты в интегрированной файловой системе. Разработчики интегрированной файловой системы стремились максимально следовать стандартам POSIX. Смешение схем прав доступа iSeries и POSIX иногда дает неожиданный эффект:

1. Не удаляйте частные права доступа пользователя к принадлежащему ему каталогу, даже если для каталога установлены достаточные общие права доступа, либо если пользователь является членом группы с нужными правами доступа или включен в список прав доступа. В стандартной модели защиты библиотек и папок сервера iSeries удаление частных прав доступа владельца сократит объем информации о правах доступа, хранящейся в пользовательском профайле, и не повлияет на другие операции. В то же время, в соответствии со стандартом POSIX при создании каталога его владелец получает такие права доступа, которые есть у владельца родительского каталога, даже если у владельца нового каталога есть другие частные права доступа к родительскому каталогу. Приведем пример, иллюстрирующий это правило. Предположим, что USERA является владельцем каталога /DIRA, но частные права доступа пользователя USERA были удалены. У USERB есть частные права доступа к /DIRA. USERB создает каталог /DIRA/DIRB. Так как у USERA нет прав доступа к объекту /DIRA, у пользователя USERB также не будет прав доступа к объекту /DIRA/DIRB. Для того чтобы пользователь USERB смог переименовать или удалить /DIRA/DIRB, придется изменить его права доступа к соответствующему объекту. Такая же ситуация возникает при создании файлов с помощью API open() с флагом O_INHERITMODE. Если пользователь USERB создаст файл /DIRA/FILEB, у него не будет ни прав доступа к этому объекту, ни прав доступа к хранящимся в нем данным. Пользователь USERB не сможет записать данные в созданный файл.
2. Принятые права доступа не поддерживаются в большинстве физических файловых систем, в том числе, в корневой файловой системе (/), в QOpenSys и в пользовательских файловых системах.
3. Объекты всегда принадлежат тому пользовательскому профайлу, который их создал, даже если в поле OWNER этого профайла указано значение *GRPPRF.
4. Для выполнения многих операций над объектами файловой системы требуются права доступа к данным *RX для каждого компонента пути, включая корневой каталог (/). В ситуациях, когда пользователю не разрешается использование объекта по причине отсутствия необходимых прав доступа, прежде всего нужно проверить, есть ли у пользователя права доступа к корневому каталогу.
5. Для просмотра содержимого или имени текущего рабочего каталога (DSPCURDIR, getcwd() и т.д.) требуются права доступа к данным *RX для каждого компонента пути. Однако для перехода к другому каталогу (CD, chdir() и т.д.) для каждого компонента пути должны быть всего лишь права доступа к данным *X. Следовательно, пользователь теоретически может перейти к каталогу, просмотр которого ему запрещен.
6. Команда COPY служит для копирования объекта. Для копии файла устанавливаются те же права доступа, что и для оригинала, за исключением прав владельца. Команда CPYTOSTMF предназначена для копирования данных. При этом у пользователя нет возможности задать права доступа к новому файлу. Владельцу (создателю) файла будут предоставлены права доступа к данным *RWX, но для группы и всех остальных пользователей будут установлены права доступа *EXCLUDE. Для назначения других прав доступа пользователю придется воспользоваться другими средствами (CHGAUT, chmod() и т.д.).
7. Информацию о правах доступа к объекту может получить только владелец этого объекта и пользователь с правами доступа *OBJMGT. Это ограничение может привести к непредвиденным сложностям, например, при вызове команды COPY,

которая должна получить информацию о правах доступа к исходному объекту для того, чтобы установить такие же права для создаваемой копии.

8. Для изменения владельца или группы объекта пользователю необходимы не только соответствующие права доступа к объекту, но и права доступа *ADD к данным профайла нового владельца или группы и права доступа *DELETE к данным профайла прежнего владельца или группы. Эти права доступа не связаны с правами доступа к файловой системе. Для просмотра прав доступа к данным применяется команда DSPOBJAUT, а для их изменения - команда EDTOBJAUT. Описанное ограничение также может привести к непредвиденным сложностям при выполнении команды COPY в момент назначения ИД группы для нового объекта.
9. При выполнении команды MOV часто возникают непредвиденные ошибки, связанные с отсутствием необходимых прав доступа. Особенно это характерно для перемещения данных из одной физической файловой системы в другую и для преобразования данных. В этих случаях перемещение объектов на самом деле является совокупностью операций копирования и удаления. Следовательно, при выполнении команды MOV нужно учитывать не только характерные для нее ограничения, но и все ограничения для команд COPY (см. пункты 7 и 8) и RMVLNK.

В следующих разделах приведена информация о ряде основных файловых систем. Сведения о других файловых системах сервера iSeries можно найти в документации по лицензионным программам, применяющим эти файловые системы.

Корневая файловая система (/), QOpenSys и пользовательские файловые системы

Ниже приведена информация о защите объектов в корневой и пользовательских файловых системах, а также в файловой системе QOpenSys.

Применение прав доступа

Корневая файловая система, QOpenSys и пользовательские файловые системы объединяют возможности сервера iSeries, PC и UNIX** как в области управления объектами, так и в области защиты. Работая в сеансе iSeries, вы можете задать все обычные для сервера iSeries права доступа к объектам с помощью команд интегрированной файловой системы (WRKAUT и CHGAUT). В их число входят права доступа *R, *W и *X, соответствующие спецификации 1170 (для операционных систем на базе UNIX).

Примечание: Корневая файловая система, QOpenSys и пользовательские файловые системы предоставляют одинаковый набор функций. В файловой системе QOpenSys учитывается регистр в именах файлов. В корневой файловой системе регистр не учитывается. В пользовательских файловых системах это настраиваемый параметр. Так как в перечисленных файловых системах применяется одинаковая схема защиты, приведенная ниже информация в равной степени относится к каждой из этих систем.

Администратор, обратившись к корневой файловой системе в сеансе PC, может задать некоторые атрибуты объектов, которые обычно применяются для ограничения доступа на персональном компьютере:

- Системный
- Скрытый
- Архивный
- Только для чтения

Эти атрибуты применяются в сочетании с правами доступа к объектам сервера iSeries, а не вместо них.

При обращении пользователя к объекту корневой файловой системы OS/400 проверяет все установленные для объекта права доступа и атрибуты, в том числе те, которые не поддерживаются пользовательским интерфейсом. Так, предположим, что для объекта установлен атрибут ″только для чтения″. Пользователь PC не может удалить такой объект с помощью интерфейса iSeries Access. Пользователь выделенной рабочей станции, подключенной к iSeries, также не сможет удалить этот объект, даже если у него есть специальные права доступа *ALLOBJ. Для удаления такого объекта пользователь должен не только получить соответствующие права доступа, но и удалить этот атрибут на PC. Точно так же, у пользователя PC может не быть достаточных прав доступа OS/400 для изменения атрибутов объекта, применяемых на PC.

Некоторые приложения сервера iSeries обращаются к объектам корневой файловой системы с помощью интерфейсов прикладных программ (API), аналогичных применяемым в операционной системе UNIX. Эти API предназначены для работы со следующими параметрами защиты:
- Владелец объекта
- Владелец группы (права доступа к основной группе в iSeries)
- Права на чтение (для файлов)
- Права на запись (изменение содержимого)
- Права на выполнение (запуск программ и поиск в каталогах)

Система преобразует эти значения в права доступа к данным и объектам, применяемые на сервере iSeries:
- Права на чтение (*R) = *OBJOPR и *READ
- Права на запись (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Права на выполнение (*X) = *OBJOPR и *EXECUTE

Аналогов других прав доступа к объектам AS/400 (*OBJMGT, *OBJEXIST, *OBJALTER и *OBJREF) в среде UNIX нет.

Однако эти права доступа определены для всех объектов корневой файловой системы. При создании объектов с помощью API, использующего схему прав доступа UNIX, объект наследует перечисленные права доступа от родительского каталога:
- Владелец нового объекта наследует права доступа к объекту от владельца родительского каталога.
- Основная группа нового объекта наследует права доступа к объекту от основной группы родительского каталога.
- Общие права доступа к объекту наследуются от родительского каталога.

Права доступа к данным для владельца, основной группы и остальных пользователей задаются в параметре режима доступа соответствующего API. Если права доступа к объекту предоставлены всем трем категориям пользователей, то будут применяться те же правила ограничения доступа, что и в UNIX. Рекомендуется предоставлять права доступа к объекту всем пользователям. В противном случае права доступа будут проверяться по схеме, применяемой в POSIX.

При работе приложения, использующего схему прав доступа UNIX, система проверяет все права доступа к объекту, в том числе те, которые не поддерживаются приложением. Например, система может применять списки прав доступа, несмотря на то, что в среде UNIX это понятие отсутствует.

Если в вашей системе работают приложения, применяющие различные схемы прав доступа, нужно учитывать, что изменение прав доступа в одной схеме может повлиять на работу тех приложений, которые применяют другую схему.

Настройка защиты в корневой файловой системе (/), QOpenSys и пользовательских файловых системах

С появлением интегрированной файловой системы на сервере iSeries был добавлен ряд команд, позволяющих работать с объектами разных файловых систем. Среди них есть команды для работы с системой защиты:

- Изменить контроль (CHGAUD)
- Изменить права доступа (CHGAUT)
- Изменить владельца (CHGOWN)
- Изменить основную группу (CHGPGP)
- Показать права доступа (DSPAUT)
- Работа с правами доступа (WRKAUT)

Эти команды преобразуют права доступа к данным и объектам в группы прав доступа, применяемые в UNIX:

***RWX** Чтение/запись/выполнение
***RW** Чтение/запись
***R** Чтение
***WX** Запись/выполнение
***W** Запись
***X** Выполнение

Кроме этого, для настройки параметров защиты можно воспользоваться API, применяющими схему прав доступа UNIX.

Общие права доступа к корневому каталогу

По умолчанию общие права доступа к корневому каталогу равны *ALL (все права доступа к объектам и данным). Это значение обеспечивает нормальную работу приложений, применяющих схему права доступа UNIX, и пользователей сервера iSeries. Если у пользователя сервера iSeries есть доступ к командной строке, то для создания новой библиотеки в файловой системе QSYS.LIB ему достаточно вызвать команду CRTLIB. Как правило, пользователям iSeries предоставляются такие права доступа. Точно так же, права доступа к корневой файловой системе, по умолчанию предоставляемые пользователю, достаточны для создания нового каталога в корневой файловой системе (подобно тому, как пользователю PC предоставляются права на создание нового каталога).

Администратор защиты должен объяснить пользователям, какие права доступа нужно устанавливать при создании объектов. При создании библиотеки рекомендуется изменить значение *CHANGE, устанавливаемое по умолчанию для общих прав доступа. В зависимости от содержимого библиотеки, пользователь должен установить общие права доступа *USE или *EXCLUDE.

Если у пользователей должна быть возможность создавать новые каталоги в корневой файловой системе (/), QOpenSys или пользовательской файловой системе, вы можете выбрать один из следующих подходов:

- Объясните пользователям, что при создании новых каталогов нужно изменять права доступа, устанавливаемые по умолчанию. Обычно права доступа наследуются от родительского каталога. В частности, если каталог создается в корневом каталоге, то по умолчанию будут установлены общие права доступа *ALL.
- Создайте специальный каталог для данных пользователей в корневом каталоге. Установите для него требуемые общие права доступа. После этого сообщите

пользователям, что все свои каталоги они должны создавать в этом специальном каталоге. При создании новых каталогов общие права доступа будут автоматически наследоваться.

- Запретите пользователям создавать объекты в корневом каталоге, установив для него соответствующие общие права доступа. (Удалите права доступа *W, *OBJEXIST, *OBJALTER, *OBJREF и *OBJMGT.) Перед изменением прав доступа проверьте, не приведет ли это к ошибкам в работе приложений. Например, это приведет к сбою в работе тех приложений, применяющих схему прав доступа UNIX, которые удаляют объекты из корневого каталога.

Команда Печать частных прав доступа к объектам (PRTPVTAUT)

Команда Печать частных прав доступа к объектам (PRTPVTAUT) выдает отчет о всех частных правах доступа, установленных для объектов определенного типа в заданной библиотеке, папке или каталоге. В отчете перечисляются все найденные объекты заданного типа и пользователи с правами доступа к этим объектам. Такой отчет позволяет узнать, каким пользователям предоставлены права доступа к объектам.

Команда выводит для выбранных объектов три отчета. Первый отчет (полный отчет) содержит список всех частных прав доступа для каждого из выбранных объектов. Второй отчет (отчет об изменениях) включает сведения о добавлении и изменении частных прав доступа к выбранным объектам. Этот отчет выдается в том случае, если команда PRTPVTAUT уже выполнялась ранее для этого же набора объектов. Отчет об изменениях содержит информацию о новых объектах заданного типа, новых правах доступа к существующим объектам и изменениях прав доступа к существующим объектам. Если команда PRTPVTAUT ранее не выполнялась для указанных объектов в заданной библиотеке, папке или каталоге, отчет об изменениях не будет создан. Если команда ранее выполнялась, но никаких изменений не произошло, отчет об изменениях будет пустым.

Третий отчет (отчет об удалении) содержит информацию об объектах и частных правах доступа к выбранным объектам, удаленных с момента предыдущего запуска команды PRTPVTAUT. Отчет об удалении включает список удаленных объектов и список пользователей, частные права доступа которых были аннулированы. Если команда PRTPVTAUT ранее не выполнялась для указанных объектов в заданной библиотеке, папке или каталоге, отчет об удалении не будет создан. Если команда ранее выполнялась, но никаких изменений не произошло, отчет об удалении будет пустым.

Ограничение: Для запуска этой команды необходимы специальные права доступа *ALLOBJ.

Примеры:

Для создания полного отчета, отчета об изменениях и отчета об удалении для всех файлов из библиотеки PAYROLLLIB вызовите следующую команду:

```
PRTPVTAUT
OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

Для создания полного отчета, отчета об изменениях и отчета об удалении для всех потоковых файлов из каталога GARRY запустите следующую команду:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

Для создания полного отчета, отчета об изменениях и отчета об удалении для всех потоковых файлов, расположенных в каталоге GARRY и всех вложенных каталогах, введите команду:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

Команда Печать объектов с общим доступом (PRTPUBAUT)

Команда Печать объектов с общим доступом (PRTPUBAUT) создает отчет о тех объектах указанного типа, для которых не установлены общие права доступа *EXCLUDE. Для объектов типа *PGM в отчет включаются только те программы, для которых не установлены общие права доступа *EXCLUDE и которые могут быть вызваны пользователем (программа принадлежит пользовательскому домену или уровень защиты системы (системное значение QSECURITY) не превышает 30). Такой отчет позволяет узнать, с какими объектами может работать любой пользователь системы.

Команда создает два отчета. Первый отчет (полный отчет) включает список всех объектов указанного типа, для которых не установлены общие права доступа *EXCLUDE. Второй отчет (отчет об изменениях) содержит список тех объектов, права доступа *EXCLUDE к которым были удалены или которые были созданы с момента предыдущего вызова команды PRTPUBAUT. Если команда PRTPUBAUT ранее не выполнялась для указанных объектов в заданной библиотеке, папке или каталоге, отчет об изменениях не будет создан. Если команда ранее выполнялось, но новых объектов без общих прав доступа *EXCLUDE не появилось, отчет об изменениях будет пустым.

Ограничение: Для запуска этой команды необходимы специальные права доступа *ALLOBJ.

Примеры:

Для создания полного отчета и отчета об изменениях для тех файлов из библиотеки GARRY, для которых не установлены общие права доступа *EXCLUDE, вызовите команду:

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

Для создания полного отчета и отчета об изменениях для потоковых файлов без общих прав доступа *EXLUDE из каталога GARRY и всех его подкаталогов, вызовите следующую команду:

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

Ограничение доступа к файловой системе QSYS.LIB

Так как корневая файловая объединяет все остальные файловые системы, QSYS.LIB выглядит как подкаталог корневого каталога. Следовательно, любой пользователь PC, которому разрешен доступ к серверу iSeries, может работать с объектами из библиотек iSeries (объектами файловой системы QSYS.LIB) с помощью обычных команд и функций PC. Например, пользователь PC может случайно удалить объект из QSYS.LIB (например, библиотеку с важными файлами).

Как описано в разделе “Корневая файловая система (/), QOpenSys и пользовательские файловые системы” на стр. 101, система проверяет все права доступа к объектам, независимо от того, поддерживаются ли они интерфейсом. Следовательно, пользователь сможет удалить объект лишь в том случае, если у него есть права

доступа *OBJEXIST. Однако если в системе iSeries ограничен доступ к меню, но не к объектам, то пользователь PC сможет удалять объекты из файловой системы QSYS.LIB.

По мере роста числа пользователей и увеличения различных способов доступа, ограничение доступа с помощью меню становится недостаточным. В разделе Глава 5, “Защита информации и права доступа к объектам”, на стр. 45 описано, каким образом средства ограничения доступа к меню можно дополнить средствами защиты объектов. Однако на сервере iSeries есть более простой способ запретить доступ к файловой системе QSYS.LIB через структуру каталогов корневой файловой системы. Создав список прав доступа QPWFSERVER, вы сможете управлять доступом пользователей к файловой системе QSYS.LIB через корневой каталог.

Если права доступа пользователя к списку прав доступа QPWFSERVER равны *EXCLUDE, то пользователь не сможет перейти в каталог QSYS.LIB из корневого каталога. Если права пользователя равны *USE, то пользователь сможет перейти в этот каталог. После перехода пользователя в каталог QSYS.LIB вступают в силу обычные права доступа к объектам этой файловой системы. Другими словами, вы можете управлять доступом ко всей файловой системе QSYS.LIB с помощью прав доступа к списку QPWFSERVER. Пользователям с правами доступа *EXCLUDE работа в этой файловой системе запрещена. Пользователям с правами доступа *USE (или выше) работа в этой файловой системе разрешена.

Обычно пользователям не требуется обращаться к объектам файловой системы QSYS.LIB через структуру каталогов. В этом случае рекомендуется установить для списка прав доступа QPWFSERVER общие права доступа *EXCLUDE. Помните, что такие права доступа запрещают доступ ко всем библиотекам в файловой системе QSYS.LIB, включая пользовательские библиотеки. Если некоторым пользователям нужно разрешить доступ к QSYS.LIB, то предоставьте им частные права доступа. Например, вы можете предоставить доступ к списку прав доступа отдельному пользователю. Однако в этом случае необходимо убедиться, что права доступа пользователя к объектам файловой системы QSYS.LIB установлены правильно. В противном случае пользователь может случайно удалить нужные объекты или целые библиотеки.

Примечания:

1. По умолчанию общие права доступа к списку прав доступа QPWFSERVER равны *USE.
2. Если вы явно предоставите права доступа отдельному пользователю, то список прав доступа будет применяться только при работе с файлами через iSeries Access, NetServer и при передаче файлов между серверами iSeries. Список прав доступа не запрещает доступ к каталогам через FTP, ODBC и другие интерфейсы.

Защита каталогов

При обращении к объекту корневой файловой системы просматриваются все каталоги, указанные в пути к этому объекту. Для просмотра каталога необходимы права доступа *X (*OBJOPR и *EXECUTE) к этому каталогу. Например, предположим, что вы обращаетесь к следующему объекту:

```
/companya/customers/custfile.dat
```

В этом случае у вас должны быть права доступа *X к каталогу `companya` и к каталогу `customers`.

В корневой файловой системе можно создавать символьные связи с объектами. По смыслу символьная связь является псевдонимом объекта. Как правило, этот

псевдоним короче полного имени объекта, поэтому его проще запомнить. При этом символьная связь не задает другой физический путь к объекту. Следовательно, если для обращения к объекту применяется символьная связь, пользователю по-прежнему нужны права доступа *X ко всем каталогам, перечисленным в пути к объекту.

Для защиты каталогов в корневой файловой системе могут применяться средства, аналогичные средствам защиты библиотек в файловой системе QSYS.LIB. Вы можете, например, установить для каталога общие права доступа *EXCLUDE, чтобы запретить пользователям обращаться к каталогу и его подкаталогам.

Защита новых объектов

Права, которые устанавливаются для нового объекта в корневой файловой системе, зависят от того интерфейса, который применялся для создания этого объекта. Например, если вы вызовете команду CRTDIR с параметрами по умолчанию, новый каталог унаследует права доступа от родительского каталога, включая частные права доступа, основную группу и списки прав доступа. В следующих разделах описываются правила предоставления прав доступа в различных интерфейсах.

Права доступа наследуются от родительского каталога, а не от каталогов, расположенных выше в иерархии. Следовательно, при настройке прав доступа к каталогам администратор защиты должен учитывать два фактора:

- Каким образом эти права доступа повлияют на доступ к объектам, расположенным в иерархии ниже текущего объекта (например, библиотеки).
- Каким образом эти права доступа отразятся на объектах, которые будут создаваться в будущем (например, параметр CRTAUT для библиотек).

Рекомендация: Если вы хотите, чтобы пользователи интегрированной файловой системы работали только в своих домашних каталогах (например, /home/usrxxx), установите соответствующие права доступа (например, PUBLIC *EXCLUDE). При создании пользователем подкаталогов в домашнем каталоге эти права доступа будут наследоваться.

Ниже описывается процедура наследования прав доступа в различных интерфейсах.

Применение команды Создать каталог

При создании каталога с помощью команды CRTDIR существует два способа задания прав доступа:

- Вы можете задать общие права доступа (к данным, объектам или к тому и другому).
- Вы можете указать *INDIR в качестве прав доступа (к данным, объектам или к тому и другому). Если в качестве прав доступа к данным и объекту указано значение *INDIR, система полностью копирует права доступа родительского каталога, включая список прав доступа, основную группу, общие права доступа и частные права доступа. (Система не копирует частные права доступа к объекту, предоставленные профайлам QSYS и QSECOFR.)

Создание каталога с помощью API

При создании каталога с помощью API mkdir() указываются права доступа к данным для владельца, основной группы и остальных пользователей (с помощью атрибутов *R, *W и *X). Права доступа к объекту наследуются от родительского каталога.

Так как в операционных системах на базе UNIX отсутствует понятие прав доступа к объекту, функция mkdir() не позволяет задать эти права доступа. Для изменения прав

доступа к объекту, установленных по умолчанию, вызовите команду CHGAUT. Учтите, что удаление некоторых прав доступа к объекту может привести к сбою в работе приложений, применяющих схему прав доступа UNIX.

Создание потокового файла с помощью API open() или creat()

При создании потокового файла с помощью API creat() указываются права доступа к данным для владельца, основной группы и остальных пользователей (с помощью атрибутов *R, *W и *X). Права доступа к объекту наследуются от родительского каталога.

Права доступа к объекту можно задать и при создании потокового файла с помощью API open(). В то же время, функция open() позволяет выбрать режим, в котором права доступа к объекту будут унаследованы от родительского каталога. Такой режим называется режимом наследования. Если вы выберете режим наследования, система полностью скопирует права доступа родительского каталога, включая список прав доступа, основную группу, общие права доступа и частные права доступа. Эта опция действует так же, как опция *INDIR команды CRTDIR.

Создание объекта с помощью интерфейса PC

Если вы создаете объект в корневой файловой системе с помощью приложения на PC, он автоматически унаследует все права доступа от родительского каталога. В число наследуемых прав доступа входят список прав доступа, основная группа, общие права доступа и частные права доступа. Приложения PC не могут самостоятельно задавать права доступа при создании объекта.

Файловая система QFileSvr.400

С помощью файловой системы QFileSvr.400 пользователь (USERX) одной системы iSeries (SYSTEMA) может обращаться к данным другой системы iSeries (SYSTEMB). Пользователю USERX предоставляется интерфейс, аналогичный интерфейсу Client Access. Удаленный сервер iSeries (SYSTEMB) будет представлен в виде каталога; файловые системы сервера будут представлены в виде подкаталогов.

При обращении пользователя USERX к системе SYSTEMB через этот интерфейс система SYSTEMA отправляет имя профайла и зашифрованный пароль пользователя USERX в систему SYSTEMB. В системе SYSTEMB должен существовать такой же профайл, иначе система отклонит запрос.

Если SYSTEMB примет запрос, то пользователь USERX будет рассматриваться системой SYSTEMB как пользователь Client Access. Ко всем действиям пользователя USERX будут применяться стандартные правила проверки прав доступа.

Администратор защиты должен знать о том, что файловая система QFileSvr.400 предоставляет еще одну возможность доступа к вашей системе. Удаленный вход в систему через меню - не единственный способ подключения к системе, доступный удаленным пользователям. Если в системе, подключенной к другой системе iSeries, активна подсистема QSERVER, то удаленные пользователи могут работать в этой системе так же, как пользователи локального PC, на котором запущена программа Client Access. Почти наверняка у вас будут соединения, для работы которых потребуется запуск подсистемы QSERVER. Это еще одна причина, по которой необходимо настроить защиту объектов с помощью прав доступа.

Сетевая файловая система

С помощью сетевой файловой системы (NFS) различные системы, поддерживающие NFS, могут обмениваться данными. NFS является стандартным способом доступа к общим ресурсам в сетях. Большинство операционных систем (включая операционные системы персональных компьютеров) поддерживают NFS. В системах UNIX NFS является основным средством доступа к данным. Сервер iSeries может работать и как клиент, и как сервер NFS.

Если вы - администратор защиты системы iSeries, выполняющей функции сервера NFS, то вы должны знать, как обеспечивается защита данных в NFS. Ниже приведены некоторые сведения и рекомендации:

- Сервер NFS запускается явным образом с помощью команды STRNFSSVR. Не забудьте ограничить права на запуск этой команды.
- Для того чтобы предоставить клиентам NFS доступ к объекту или каталогу, его надо `экспортировать`. Следовательно, вы можете четко определить компоненты системы, доступные клиентам NFS.
- При экспорте объектов можно задать список клиентов, которым разрешен доступ к этим объектам. Клиенты идентифицируются по именам систем или IP-адресам. Клиентом может быть как персональный компьютер, так и сервер iSeries или система UNIX. В NFS клиент (IP-адрес) называется `машиной`.
- Любой машине, которая будет работать с экспортируемыми ресурсами, можно предоставить права на чтение и запись или только на чтение. В большинстве случаев рекомендуется предоставлять права только на чтение.
- NFS не обеспечивает проверки паролей. Эта файловая система предназначена для работы с общими данными внутри защищенной сети. В запросе на доступ к системе сервер получает идентификатор пользователя (`uid`). Этот `uid` применяется для следующих целей:
  - Сервер iSeries выполняет поиск пользовательского профайла с тем же `uid`. Если такой профайл будет найден, `uid` предоставляется временное разрешение с правами доступа этого профайла. Временное разрешение - это термин NFS, описывающий набор прав доступа пользователя. Предоставление временного разрешения аналогично замене профайла в других приложениях сервера iSeries.
  - При экспорте каталога или объекта можно указать, разрешен ли доступ к этому объекту профайлу с правами root. Сервер NFS для iSeries преобразует права доступа root в специальные права доступа *ALLOBJ. Если профайлу с правами root доступ запрещен, то он будет запрещен всем пользователям NFS, `uid` которых соответствует пользовательскому профайлу со специальными правами доступа *ALLOBJ. Если в системе разрешен анонимный доступ, то с таким пользователем будет связан анонимный профайл.
  - При экспорте каталога или объекта можно указать, разрешены ли анонимные запросы. Анонимный запрос - это запрос с `uid`, не соответствующим ни одному из `uid`, определенных в системе. Если анонимный доступ разрешен, то анонимными пользователям будет предоставляться профайл QNFSANON, поставляемый фирмой IBM. У этого пользовательского профайла отсутствуют специальные или частные права доступа. (При экспорте можно задать другой профайл для обработки анонимных запросов.)
- Если сервер iSeries подключен к сети NFS (в которой присутствуют системы UNIX, использующие `uid`), то вам, вероятно, потребуется вручную создать список `uid`. Это связано с тем, что набор `uid` должен быть согласован между всеми системами сети.

  Возможно, вам потребуется изменить некоторые `uid` (даже в профайлах, поставляемых фирмой IBM) для совместимости с другими системами в сети. Для

изменения uid можно воспользоваться специальной программой, значительно упрощающей всю процедуру. (Одновременно с изменением uid пользовательского профайла нужно изменить uid владельца для всех объектов, принадлежащих этому профайлу и расположенных в корневом каталоге или каталоге QOpenSrv.) Программа QSYCHGID позволяет автоматически изменить uid в пользовательском профайле и описаниях принадлежащих ему объектов. Информация о работе с этой программой приведена в книге *iSeries System API Reference*.

Глава 12. Защита соединений APPC

После подключения системы к сети у пользователей появляется множество новых возможностей по работе с ней. Администратор защиты должен знать обо всех средствах управления доступом к системе в сети APPC.

Расширенные средства межпрограммной связи (APPC) - это протокол связи, с помощью которого компьютеры, в том числе PC, могут обмениваться данными. Соединения APPC могут применяться такими функциями, как удаленный вход в систему дисплейной станции, управление распределенными данными и iSeries Access для Windows.

В следующих разделах приведена основная информация о соединениях APPC и средствах их защиты. В первую очередь рассматриваются опции защиты, которые можно задать в конфигурации APPC. Для того чтобы реализовать приведенные примеры на своем компьютере, вам потребуется помощь администратора сети, а в некоторых случаях и поставщиков приложений. Эта информация может служить основой для анализа различных средств и функций защиты APPC.

Применение средств защиты всегда связано с “накладными расходами”. Обычно упрощение защиты сети приводит к усложнению ее администрирования. Например, в этом документе не рассматриваются сети на базе протокола APPN (Расширенное равноправное сетевое взаимодействие), так как принципы защиты проще объяснить без применения APPN. Однако, если APPN не применяется, то администратор сети должен вручную создавать информацию о конфигурации, которую APPN создает автоматически.

Соединения с PC

Многие способы подключения PC к серверу iSeries зависят от выбранного протокола связи, например, APPC или TCP/IP. При чтении следующих разделов подумайте, какие средства защиты можно задействовать с различными способами соединения с другими системами и PC. Ваш план защиты сети не должен отрицательно сказываться на работе PC, подключенных к системе.

Терминология APPC

APPC позволяет пользователю одной системы работать в другой системе. Систему, из которой передаются запросы на выполнение операций, принято называть следующим образом:

- **Исходная система**
- **Локальная система**
- **Клиент**

Систему, принимающую запросы, принято называть следующим образом:

- **Целевая система**
- **Удаленная система**
- **Сервер**

Этапы настройки соединения APPC

С точки зрения системного администратора, перед тем, как пользователь одной системы (SYSTEMA) сможет работать в другой системе (SYSTEMB), должны быть выполнены следующие действия:

- Исходная система (SYSTEMA) должна настроить канал связи с целевой системой (SYSTEMB). Этот канал связи называется **сеансом APPC**.
- Целевая система должна идентифицировать пользователя и связать его с пользовательским профайлом. Целевая система должна поддерживать алгоритм шифрования исходной системы (подробнее см. “Уровни паролей” на стр. 16).
- Целевая система должна запустить для пользователя задание в соответствующей среде (определяемой параметрами управления заданием).

Более подробно эти этапы и способы защиты, применяемые на каждом из них, описаны ниже. Основная ответственность за защиту соединения APPC ложится на администратора защиты целевой системы. Однако согласованная работа обоих администраторов значительно упростит задачу настройки защиты APPC.

Пример: Сеанс APPC

Когда пользователь одной системы пытается обратиться к другой системе в среде APPC, открывается сеанс работы этих систем. Для того чтобы открыть сеанс, необходимо установить соединение между двумя устройствами APPC. Имя удаленного расположения (параметр RMTLOCNAME) в описании устройства APPC системы SYSTEMA должно совпадать с именем локального расположения (параметр LCLLOCNAME) в описании устройства APPC системы SYSTEMB, и наоборот.

Для того чтобы две системы могли установить между собой сеанс APPC необходимо, чтобы совпадали пароли для доступа к удаленному расположению в описаниях устройств APPC этих систем. Либо оба пароля должны быть не заданы, либо они должны быть равны.

Если пароли заданы, они хранятся и передаются в зашифрованном виде. Если пароли совпадают, то между системами устанавливается сеанс. Если пароли не совпадают, запрос пользователя отклоняется. Если в ходе установления сеанса проверяются пароли расположения, то такая процедура называется **защищенным связыванием**.

Примечание: Функция защищенного связывания поддерживается не всеми компьютерными системами.

Ограничение доступа к сеансам APPC

Для управления доступом к другим системам проще всего задать нужные права доступа к объектам исходной системы. Установите для описаний устройств APPC общие права доступа *EXCLUDE, а права доступа *CHANGE предоставьте лишь тем пользователям, кому это нужно. Для того чтобы запретить пользователям с правами *ALLOBJ доступ к соединениям APPC, установите соответствующее системное значение QLMTSECOFR.

Администратор защиты целевой системы может запретить пользователям запускать сеансы APPC, задав соответствующие права доступа к устройствам APPC. При этом следует проанализировать, каким пользователям требуется доступ к описанию устройства APPC. Информация о том, как сервер iSeries связывает ИД пользователя с сеансом APPC, приведена в разделе “Организация доступа пользователей APPC в целевую систему” на стр. 113.

Примечание: Для того чтобы узнать, каким пользователям системы предоставлен доступ к описаниям устройств, воспользуйтесь командой Напечатать объекты, доступные всем пользователям (PRTPUBAUT *DEVD) или командой Напечатать частные права доступа (PRTPVTAUT *DEVD).

Если в системе применяется APPN, то при отсутствии устройств для заданного маршрута автоматически создается новое устройство APPN. . Один из способов ограничения доступа к устройствам APPC в системе APPN заключается в создании списка прав доступа. Список прав доступа - это список пользователей, которым разрешен доступ к устройствам APPC. Для изменения команды CRTDEVAPPC нужно вызвать команду Изменить значения параметров команды по умолчанию (CHGCMDDFT). В качестве значения по умолчанию для параметра AUT (Права доступа) команды CRTDEVAPPC укажите созданный список прав доступа.

Примечание: Если в системе применяется язык, отличный от английского, эту процедуру нужно проделать для всех национальных языков (в соответствующих библиотеках QSYSxxxx).

Для идентификации системы, пытающейся установить сеанс с локальной системой (от имени пользователя или приложения), применяется пароль расположения (параметр LOCPWD). Проверка пароля расположения позволяет удостовериться в подлинности удаленной системы.

Если вы планируете применять пароль расположения, вам необходимо согласовать его с администраторами защиты других систем сети. Вы также можете ограничить число пользователей, которым разрешено создавать и изменять описания устройств APPC. Для вызова команд, предназначенных для работы с устройствами APPC и списками конфигураций APPN, необходимы специальные права доступа *IOSYSCFG.

Примечание: Пароли приложений для сети APPN хранятся в списке конфигураций QAPPNRMT, а не в описаниях устройств.

Организация доступа пользователей APPC в целевую систему

После установления сеанса APPC между двумя системами создается маршрут, по которому будут передаваться запросы пользователя в целевую систему. Действия, которые должен выполнить пользователь для входа в целевую систему, зависят от нескольких факторов.

Эти факторы описаны в следующем разделе.

Способы передачи информации о пользователе

В архитектуре APPC предусмотрено три способа передачи идентификационной информации из исходной системы в целевую систему. Эти способы называются **архитектурными значениями защиты**. Они описаны в Табл. 18.

Примечание: Дополнительная информация об архитектурных значениях защиты приведена в книге *APPC Programming*.

Таблица 18. Уровни защиты в архитектуре APPC

Уровень защиты	Передается ли ИД пользователя	Передается ли пароль пользователя
None	Нет	Нет
Same	Да[1]	См. примечание 2.

Таблица 18. Уровни защиты в архитектуре APPC (продолжение)

Уровень защиты	Передается ли ИД пользователя	Передается ли пароль пользователя
Program	Да	Да[3]

Примечания:

1. Исходная система передает ИД пользователя в целевую систему, если в целевой системе указано значение SECURELOC(*YES) или SECURELOC(*VFYENCPWD).
2. При отправке запроса пользователь не вводит пароль, так как он уже проверен исходной системой. Если указано значение SECURELOC(*YES) или SECURELOC(*NO), исходная система не отправляет пароль. Если указано SECURELOC(*VFYENCPWD), исходная система отправляет сохраненный зашифрованный пароль.
3. Если исходная и целевая системы поддерживают функцию шифрования паролей, то пароль отправляется в зашифрованном виде. В противном случае пароль не шифруется.

Архитектурное значение защиты устанавливается в зависимости от приложения, запрошенного пользователем. Например, для SNADS всегда применяется значение SECURITY(NONE), а для DDM - значение SECURITY(SAME). Для удаленного входа в систему дисплейной станции пользователь может выбрать значение защиты с помощью команды STRPASTHR.

В любом случае целевая система решает, нужно ли принимать запрос с тем значением защиты, которое задано в исходной системе. В некоторых случаях целевая система может полностью отклонить запрос. В других случаях она может принудительно установить другое значение защиты. Например, если пользователь задал в команде STRPASTHR ИД и пароль, то для запроса будет установлено значение защиты SECURITY(PGM). Однако если в целевой системе системное значение QRMTSIGN равно *FRCSIGNON, пользователю все равно будет выдано меню Вход в систему. Если задано значение *FRCSIGNON, система всегда применяет значение SECURITY(NONE), что равносильно вызову команды STRPASTHR без указания ИД пользователя и пароля.

Примечания:

1. Перед отправкой данных исходная и целевая системы согласуют значение защиты. Например, если целевая система указала SECURELOC(*NO), а в запросе задано SECURITY(SAME), целевая система принудительно устанавливает значение SECURITY(NONE). Исходная система не передает ИД пользователя.
2. Целевая система отклоняет запрос на установление сеанса, если срок действия пароля пользователя истек. Это относится только к запросам на подключение, содержащим пароль, и в том числе:
   - К запросам на установление сеанса типа SECURITY(PROGRAM).
   - К запросам на установление сеанса типа SECURITY(SAME), если значение SECURELOC равно *VFYENCPWD.

Распределение функций защиты

Если система подключена к сети, вы должны решить, можно ли возложить ответственность за идентификацию пользователей, подключающихся к вашей системе, на другие системы сети. Будет ли достаточно, если SYSTEMA проверит, что пользователь USERA - это действительно USERA (а пользователь QSECOFR - это действительно QSECOFR)? Или же вы будете еще раз запрашивать у пользователей ИД и пароль?

Значение параметра SECURELOC (защищенное расположение) в описании устройства APPC целевой системы указывает, доверяете ли вы исходной системе (защищена ли она).

Если в обеих системах установлен выпуск, поддерживающий значение *VFYENCPWD, то с помощью параметра SECURELOC(*VFYENCPWD) можно обеспечить дополнительную защиту приложений, применяющих значение SECURITY(SAME). Хотя пользователь не вводит пароль при отправке запроса, исходная система отправляет вместе с запросом сохраненный пароль пользователя. Для того чтобы запрос был принят целевой системой, пользователю должны быть назначены одни и те же идентификатор и пароль в обеих системах.

Если целевая система укажет SECURELOC(*VFYENCPWD), а исходная система не поддерживает это значение, будет установлено значение SECURITY(NONE).

В Табл. 19 описаны различные сочетания архитектурных значений защиты и значений SECURELOC:

Таблица 19. Результат применения уровня защиты APPC совместно со значением SECURELOC

Исходная система	**Целевая система**	
Уровень защиты	**Значение SECURELOC**	**Пользовательский профайл для задания**
None	Любое	Пользователь по умолчанию[1]
Same	*NO	Пользователь по умолчанию[1]
	*YES	Профайл пользователя исходной системы, отправившего запрос
	*VFYENCPWD	Профайл пользователя исходной системы, отправившего запрос. В обеих системах у пользователя должен быть один и тот же пароль.
Program	Любое	Профайлы пользователей, указанные в запросе исходной системы.

Примечания:

1. Пользователь по умолчанию указывается в записи средств связи в описании подсистемы. Дополнительная информация приведена в разделе “Выбор пользовательского профайла для задания в целевой системе”.

Выбор пользовательского профайла для задания в целевой системе

С каждым запросом на запуск задания APPC в другой системе связано имя режима. Имя режима указывается в запросе пользователя, а если его нет, то применяется значение по умолчанию из сетевых атрибутов исходной системы.

В зависимости от имени режима и имени устройства APPN целевая система выбирает способ выполнения задания. Она просматривает записи средств связи в активных подсистемах и выбирает ту, которая больше всего соответствует заданному имени устройства APPN и имени режима.

Запись средств связи содержит имя пользовательского профайла, который будет применяться для запросов SECURITY(NONE). Ниже приведен пример записи средств связи в описании подсистемы:

```
                        Показать записи средств связи

Описание подсистемы:     QCMN          Состояние:   ACTIVE

                          Описание                    Пользов.      Макс.
Устройство    Режим       задания       Библиотека    по умолч.     продолж.
                                                                    работы
*ALL          *ANY        *USRPRF                     *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                     *NONE         *NOMAX
```

В Табл. 20 показаны возможные значения параметра, задающего пользователя по умолчанию в записи средств связи:

Таблица 20. Возможные значения параметра, задающего пользователя по умолчанию

Значение	Действие
***NONE**	Пользователь по умолчанию не определен. Если в запросе исходной системы не будет задан ИД пользователя, задание не будет запущено.
***SYS**	Будут запускаться только программы, поставляемые фирмой IBM (системные задания). Пользовательские приложения запускаться не будут.
имя-пользователя	Если в запросе исходной системы не будет задан ИД пользователя, задание будет выполняться под управлением указанного пользовательского профайла.

Для того чтобы напечатать список всех подсистем, в которых задана запись средств связи с именем пользователя по умолчанию, выполните команду Печать описания подсистемы (PRTSBSDAUT).

Параметры удаленного входа в систему дисплейной станции

Функция удаленного входа в систему дисплейной станции может служить примером приложения, применяющего протокол APPC. Эта функция предназначена для входа в другую систему, подключенную к той же сети.

Примеры запросов на удаленный вход в систему (команда STRPASTHR) и описание процедуры обработки этих запросов в целевой системе приведены в Табл. 21 на стр. 117. Для удаленного входа в систему дисплейной станции применяются основные средства протокола APPC и системное значение удаленного входа в систему (QRMTSIGN).

Примечание: Запросы на удаленный вход в систему дисплейной станции больше не направляются в подсистемы QCMN и QBASE. Начиная с версии V4R1, они направляются в подсистему QSYSWRK. В версиях младше V4R1 функция удаленного входа в систему дисплейной станции работала только в случае, если была запущена подсистема QCMD или QBASE. В более старших версиях это не так. Вы можете принудительно направить все запросы на удаленный вход в систему в подсистему QCMN (или QBASE, если она активна), изменив системное значение QPASTHRSVR на 0.

Таблица 21. Примеры запросов на удаленный вход в систему

Параметры команды STRPASTHR		**Целевая система**		
ИД пользователя	**Пароль**	**Значение SECURELOC**	**Значение QRMTSIGN**	**действие**
*NONE	*NONE	Любое	Любое	Пользователь должен войти в целевую систему.
Имя пользовательского профайла	Не задан	Любое	Любое	Запрос не будет выполнен.
*CURRENT	Не задан	*NO	Любое	Запрос не будет выполнен
		*YES	*SAMEPRF	Интерактивное задание запускается под управлением пользовательского профайла с тем же именем, что и в исходной системе. Пароль в удаленную систему не передается.В целевой системе должен быть определен такой пользовательский профайл.
			*VERIFY	
			*FRCSIGNON	Пользователь должен войти в целевую систему.
		*VFYENCPWD	*SAMEPRF	Интерактивное задание запускается под управлением пользовательского профайла с тем же именем, что и в исходной системе. Исходная система получает пароль пользователя и отправляет его в удаленную систему. В целевой системе должен быть определен такой пользовательский профайл.
			*VERIFY	
			*FRCSIGNON	Пользователь должен войти в целевую систему.
*CURRENT (или имя пользовательского профайла, под управлением которого выполняется задание)	Задан	Любое	*SAMEPRF	Интерактивное задание запускается под управлением пользовательского профайла с тем же именем, что и в исходной системе. Пароль *передается* в удаленную систему. В целевой системе должен быть определен такой пользовательский профайл.
			*VERIFY	
			*FRCSIGNON	Пользователь должен войти в целевую систему.

Таблица 21. Примеры запросов на удаленный вход в систему (продолжение)

Параметры команды STRPASTHR		**Целевая система**		
ИД пользователя	**Пароль**	**Значение SECURELOC**	**Значение QRMTSIGN**	**действие**
Имя пользовательского профайла (имя, отличное от текущего пользовательского профайла задания)	Задан	Любое	*SAMEPRF	Запрос не будет выполнен.
			*VERIFY	Интерактивное задание запускается под управлением пользовательского профайла с тем же именем, что и в исходной системе. Пароль *передается* в удаленную систему. В целевой системе должен быть определен такой пользовательский профайл.
			*FRCSIGNON	Будет запущено интерактивное задание под управлением указанного пользовательского профайла. Пароль передается в целевую систему. Указанный пользовательский профайл должен быть определен в целевой системе.

Предотвращение несанкционированного доступа

Если на активном устройстве происходит сбой, система пытается возобновить его работу. В некоторых случаях при разрыве соединения другой пользователь без прав доступа может попытаться возобновить прерванный сеанс. Предположим, что пользователь USERA выключил рабочую станцию, не выйдя из системы. В этом случае пользователь USERB может включить рабочую станцию и перезапустить сеанс пользователя USERA, не входя в систему.

Для того чтобы таких ситуаций не возникало, установите системное значение Действие при ошибке устройства I/O (QDEVRCYACN) равным *DSCMSG. В этом случае при сбое устройства система будет завершать задание пользователя.

Управление удаленными командами и пакетными заданиями

Ниже описано несколько способов ограничить набор удаленных команд и заданий, которые разрешено запускать в системе:

- Если в системе применяется DDM, вы можете ограничить доступ к файлам DDM, для того чтобы запретить пользователям других систем выполнять команду Запустить удаленную команду (SBMRMTCMD). Для запуска команды SBMRMTCMD у пользователя должны быть права на открытие файла DDM. Кроме того, вы должны ограничить число пользователей, у которых есть права на создание файлов DDM.
- В системном значении Обработка запросов DDM (DDMACC) можно задать программу выхода. Эта программа могла бы проверять все запросы DDM перед их обработкой.
- Сетевой атрибут Действие над сетевым заданием (JOBACN) можно установить таким образом, чтобы запретить обычный или автоматический запуск сетевых заданий.

- Кроме того, можно явно задать программы, которые разрешено запускать по сети, удалив запись маршрутизации PGMEVOKE из описания подсистемы. Запись маршрутизации PGMEVOKE позволяет задать выполняемые программы для инициатора запроса. После удаления этой записи маршрутизации из описаний подсистем, в том числе из QCMN, вы должны добавить записи маршрутизации для тех удаленных запросов, которым разрешено выполняться.

  В “Запросы архитектурного TPN” на стр. 93 перечислены имена программ для запросов на запуск приложений, поставляемых фирмой IBM. Для всех запросов, которые разрешено выполнять, нужно добавить записи маршрутизации, указав в качестве значения для сравнения имя программы.

  Прежде чем выполнять указанные действия, рекомендуем вам ознакомиться со средой управления заданиями и описаниями различных типов запросов. После изменения записей маршрутизации нужно убедиться, что запросы всех типов обрабатываются правильно. В случае, если системе не удается найти запись маршрутизации для запроса на подключение, выдается сообщение CPF1269. Вместо описанного способа защиты можно установить общие права доступа *EXCLUDE для тех программ транзакций, которые не должны запускаться в системе.

  Примечание: Дополнительная информация о записях маршрутизации и обработке запросов на запуск программ приведена в книге *Work Management*.

Анализ конфигурации APPC

Для просмотра списка значений параметров конфигурации APPC, влияющих на надежность защиты, вызовите команду PRTCMNSEC (Печать параметров защиты средств связи). Ниже приведены описания отчетов, которые можно получить с помощью этой команды.

Параметры устройств APPC, на которые следует обратить внимание

На рис. 9 показан пример отчета Информация о средствах связи, содержащего сведения об описаниях устройств. На рис. 10 на стр. 120 показан пример отчета, содержащего информацию о списках конфигураций. Описание полей отчетов приведено ниже.

```
                Информация о средствах связи (полный отчет)
                                                                    SYSTEM4
Тип объекта  . . . . . . . . . :   *DEVD

                                                                              Предв.      Запуск
Имя             Тип             Категория       Защищенное    Пароль        Поддержка   Одиночный   открывать   программы
объекта         объекта         устройства      располож.     располож.      APPN       сеанс       сеанс        SNUF

CDMDEV1         *DEVD           *APPC             *NO           *NO          *NO          *YES         *NO
CDMDEV2         *DEVD           *APPC             *NO           *NO          *NO          *YES         *NO
```

Рисунок 9. Описания устройств APPC - Пример отчета

```
                  Показать список конфигураций                    Страница 1
                              SYSTEM4  12/17/95  07:24:36
Список конфигураций. . . . . . . . :   QAPPNRMT
Тип списка конфигураций  . . . . . :   *APPNRMT
Текст. . . . . . . . . . . . . . . :
--------------Удаленные расположения APPN---------------
          ИД                  Удал.     ИД сети
Удаленное удаленной Локальное управл.   управл.   Защищ.
располож. сети      располож. точка     точки     располож.
SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN       *NO
SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN       *NO
SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN       *YES
SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN       *NO
SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN       *NO
----------------------Удаленные расположения APPN-------------------------
          ИД                                          Локальн.  Предварительно
Удаленное удаленной Локальное Одиночный     Число     управл.   открывать
располож. сети      располож. сеанс        диалогов   точка      сеанс
SYSTEM36  APPN      SYSTEM4    *NO             10      *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO             10      *NO        *NO
```

Рисунок 10. Список конфигураций - Пример отчета

Параметр Защищенное расположение

Значение в поле Защищенное расположение (SECURELOC) показывает, может ли проверка пароля выполняться не локальной, а удаленной системой. Параметр SECURELOC устанавливается только для приложений, которые используют значение SECURITY(SAME) (например, для DDM и API Общий программный интерфейс связи).

Если вы укажете SECURELOC(*YES), то безопасность системы будет зависеть от надежности защиты удаленной системы. Как локальные, так и удаленные пользователи смогут запускать программы в системе. Это опасно, в частности, из-за того, что во всех системах iSeries существует профайл QSECOFR (системный администратор) со специальными правами доступа *ALLOBJ. И если в какой-то системе сети не предусмотрена надежная защита пароля QSECOFR, то для остальных систем сети, считающих эту систему защищенной, существует угроза несанкционированного доступа.

Если будет задано значение SECURELOC(*VFYENCPWD), система будет менее чувствительной к тому, насколько надежно защищены пароли в других системах. У пользователя, обращающегося к приложению с параметром SECURITY(SAME), в обеих системах должен быть один и тот же идентификатор и пароль. В случае SECURELOC(*VFYENCPWD) требуется, чтобы во всей сети применялась единая стратегия управления паролями, в соответствии с которой у пользователя во всех системах будет один и тот же пароль.

Примечание: Значение SECURELOC(*VFYENCPWD) поддерживается только при установлении соединения между системами с операционной системой версии V3R2, V3R7 или V4R1. Если в целевой системе задан параметр SECURELOC(*VFYENCPWD), но исходная система не поддерживает это значение, то будет установлено значение SECURITY(NONE).

Если в системе задан параметр SECURELOC(*NO), то для запуска приложений, применяющих значение SECURITY(SAME), должен быть определен пользователь по умолчанию. Пользователь по умолчанию выбирается в зависимости от описания

устройства и режима, связанных с запросом. (См. “Выбор пользовательского профайла для задания в целевой системе” на стр. 115.)

Параметр Пароль расположения

В поле Пароль расположения указывается, должны ли системы обмениваться паролями и проверять, что соответствующая удаленная система не выдает себя за другую систему. Подробная информация о паролях расположений приведена в разделе “Пример: Сеанс APPC” на стр. 112.

Параметр Поддержка APPN

Значение в поле Поддержка APPN (APPN) указывает, поддерживает ли удаленная система функции расширенного сетевого взаимодействия, или же она поддерживает только соединения с соседними узлами. APPN(*YES) означает следующее:

- Если удаленная система - узел сети, то она может применяться для подключения локальной системы к другим системам сети. Это называется **маршрутизацией через промежуточные узлы**. При этом пользователи локальной системы могут использовать удаленную систему как маршрутизатор для подключения к сети большего размера.
- Если локальная система - узел сети, то удаленная система может подключаться к другим системам сети через эту систему. Пользователи удаленной системы могут применять локальную систему как маршрутизатор для подключения к сети большего размера.

Примечание: Для того чтобы узнать, какой тип узла представляет данная система (конечный или сетевой), вызовите команду DSPNETA.

Параметр Одиночный сеанс

Значение в поле Одиночный сеанс (SNGSSN) указывает, может ли удаленная система поддерживать несколько сеансов одновременно с помощью одного и того же описания устройства APPC. Обычно применяется значение SNGSSN(*NO), поскольку при этом для удаленной системы не нужно создавать несколько описаний устройств. Например, пользователю PC часто требуется несколько сеансов эмуляции 5250, а также сеансы для работы с файловым сервером и сервером печати. Если вы укажете SNGSSN(*NO), то все эти сеансы могут быть установлены с помощью одного описания устройства, выделенного для соединения системы iSeries с PC.

Однако указав это значение вам придется полагаться на то, что ни пользователи PC, ни другие пользователи APPN не будут пытаться нарушить защиту системы. Это связано с тем, что удаленный пользователь без соответствующих прав доступа потенциально может открыть сеанс с помощью того описания устройства, которое уже применяется в одном из существующих сеансов. (Такой вид несанкционированного доступа иногда называется **маскировкой**.)

Параметр Предварительно открывать сеанс

Для устройства в режиме одиночного сеанса значение параметра Предварительно открывать сеанс (PREESTSSN) указывает, открывает ли локальная система сеанс связи с удаленной системой, когда удаленная система подключается первой. Если задано PREESTSSN(*NO), то локальная система не запускает сеанс и ждет, пока сеанс с данной системой не будет запрошен приложением. Значение PREESTSSN(*YES) позволяет уменьшить время, требующееся приложению для установления соединения.

Значение PREESTSSN(*YES) запрещает системе отключать коммутируемую линию, которая больше не используется. Линия должна отключаться явным образом (либо пользователем, либо приложением). Если задано PREESTSSN(*YES), то

увеличивается время, в течение которого сохраняется возможность входа в локальную систему ″замаскированного″ пользователя без достаточных прав доступа.

Параметр Запуск программы SNUF

Поле Запуск программы SNUF указывает, разрешено ли удаленной системе запускать программы в локальной системе. Если задано значение *YES, то в локальной системе должна быть создана схема прав доступа к объектам, защищающая объекты от заданий и программ, запущенных удаленными пользователями.

Параметры контроллеров APPC

На рис. 11 приведен пример отчета Информация о средствах связи, содержащего сведения об описаниях контроллеров. Описания полей отчета приведены далее.

```
                    Информация о средствах связи (полный отчет)
                                                                    SYSTEM4
Тип объекта  . . . . . . . . . . :   *CTLD

Имя       Тип       Категория    Создавать  Контроллер    Тип     Поддержка   Сеансы       Таймер     Время    Имя
объекта   объекта   контроллера  автомат.   комм.линии   вызова     APPN        CP        отключения  до откл. устройства
CTL01     *CTLD     *APPC         *YES       *YES        *DIAL     *YES        *YES           0        1440    AARON
CTL02     *CTLD     *APPC         *YES       *YES        *DIAL     *YES        *YES           0        1440    BASIC
CTL03     *CTLD     *APPC         *YES       *YES        *DIAL     *YES        *YES           0        1440    *NONE
```

Рисунок 11. Описания контроллеров APPC - Пример отчета

Параметр автоматического создания устройства

Параметр AUTOCRTCTL (Создавать автоматически) описания линии определяет, должна ли локальная система автоматически создавать описание контроллера, если для полученного запроса не найдено соответствующее описание контроллера. Параметр AUTOCRTDEV (Создавать автоматически) описания устройства определяет, должна ли локальная система автоматически создавать описание устройства, если для полученного запроса не найдено соответствующее описание устройства.

Для контроллеров с поддержкой APPN это поле игнорируется. Система автоматически создает описания таких устройств, независимо от значения параметра Создавать автоматически.

Если для описания линии будет указано значение *YES, то к системе сможет подключиться любой пользователь, у которого есть права доступа к линии. Это же относится и к подключению через мосты и маршрутизаторы.

Параметр Сеансы управляющей точки

Для контроллеров с поддержкой APPN поле Сеансы управляющей точки (CPSSN) определяет, должно ли соединение APPC с удаленной системой устанавливаться автоматически. Сеанс управляющей точки (CP) используется системой для обмена информацией о сети и о состоянии с удаленной системой. Своевременная рассылка обновлений по сети APPN необходима для правильной работы сетевых функций.

Значение *YES запрещает автоматическое отключение простаивающей коммутируемой линии. При этом ваша система становится уязвимой, так как доступ к ней может получить ″замаскированный″ пользователь.

Параметр Таймер отключения

Таймер отключения задает максимальное время простоя контроллера APPC, по истечении которого система отключает линию связи с удаленной системой. Это поле имеет два значения. Первое значение определяет, сколько времени контроллер будет

оставаться активным с момента первого подключения. Второе значение задает интервал времени после завершения последнего сеанса, по истечении которого система отключает линию с данным контроллером.

Таймер отключения используется системой только в том случае, если в поле Отключение коммутируемого соединения (SWTDSC) задано значение *YES.

Если в этом поле будут указаны большие значения, то система станет уязвимой для ″замаскированных″ пользователей.

Параметры описания линии

На рис. 12 показан пример отчета Информация о средствах связи, содержащего сведения об описаниях линий. Описания полей отчета приведены далее.

```
                    Информация о средствах связи (полный отчет)

Тип объекта  . . . . . . . . . :   *LIND
Имя
авто-          Тип           Категория     Создавать   Время до    Автом.     Авт. набор
объекта        объекта       линии         автомат.    откл., с    ответ      номера
LINE01          *LIND         *SDLC           *NO           0       *NO       *NO
LINE02          *LIND         *SDLC           *NO           0       *YES      *NO
LINE03          *LIND         *SDLC           *NO           0       *NO       *NO
LINE04          *LIND         *SDLC           *NO           0       *YES      *NO
```

Рисунок 12. Описания линий APPC - Пример отчета

Параметр Автоматический ответ

Значение в поле Автоматический ответ (AUTOANS) определяет, будет ли коммутируемая линия принимать поступающие вызовы без вмешательства оператора.

Если вы укажете значение *YES, то защита будет менее надежной, а система - более уязвимой. Для того чтобы свести к минимуму вероятность несанкционированного доступа к системе, вы должны отключать линию, когда она вам не нужна.

Параметр Автоматический набор номера

Значение в поле Автоматический ответ (AUTODIAL) определяет, может ли коммутируемая линия отправлять вызовы без вмешательства оператора. Если указать значение *YES, то локальные пользователи, у которых нет физического доступа к линиям связи и модемам, смогут подключаться к другим системам.

Глава 13. Защита соединений TCP/IP

TCP/IP - это стандартный протокол связи, который применяется компьютерами различных типов для обмена данными. Приложения TCP/IP широко используются для “передачи информации по сетевым соединениям”.

В этом разделе приведена информация по следующим вопросам:

- Запрещение запуска приложений TCP/IP в системе.
- Защита ресурсов системы, в которой разрешен запуск приложений TCP/IP.

Полная информация обо всех приложениях TCP/IP приведена в разделе iSeries Information Center—>Сеть—>TCP/IP. В документе *SecureWay: iSeries u Internet* (iSeries Information Center—>Защита—>SecureWay) приведены рекомендации по защите соединений сервера iSeries с Internet (большой сетью TCP/IP) и внутренней сетью. Информация о работе со справочной системой iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Обратите внимание, что сервер iSeries поддерживает многие приложения TCP/IP. Если вы разрешите запуск одного приложения TCP/IP, вы можете неявно разрешить запуск и других приложений TCP/IP. Администратор защиты должен иметь представление обо всех приложениях TCP/IP, а также об угрозах безопасности системы, связанных с запуском этих приложений.

Настройка запрета на запуск приложений TCP/IP

Задания серверов TCP/IP выполняются в подсистеме QSYSWRK. Для запуска TCP/IP в системе применяется команда Запустить TCP/IP (STRTCP). Если вы не хотите, чтобы в системе выполнялись задания и приложения TCP/IP, не запускайте команду STRTCP. По умолчанию общие права доступа к команде STRTCP равны *EXCLUDE.

Если вы предполагаете, что один из пользователей, у которых есть права на выполнение этой команды, запускает TCP/IP (например, в нерабочее время), включите функцию контроля за доступом к команде STRTCP. В этом случае при запуске команды система будет заносить запись в журнал контроля.

Функции защиты TCP/IP

Для создания более надежной и гибкой схемы защиты сети могут применяться функции защиты TCP/IP. Хотя некоторые из функций защиты TCP/IP, входящих в состав OS/400, предусмотрены в программах брандмауэра, они не предназначены для использования в качестве брандмауэра. Тем не менее, в некоторых случаях они могут применяться для защиты вместо брандмауэра. Помимо этого, функции TCP/IP могут применяться в качестве дополнительных средств защиты в сетях с брандмауэром.

Вы можете усилить защиту TCP/IP с помощью следующих утилит:

- Правила обработки пакетов
- HTTP Proxy Server
- VPN (виртуальная частная сеть)
- SSL

Применение правил обработки пакетов для защиты соединений TCP/IP

Правила обработки пакетов, в состав которых входят правила фильтрации пакетов IP и правила преобразования сетевых адресов (NAT), играют роль брандмауэра, который запрещает посторонним доступ во внутреннюю сеть. Правила фильтрации пакетов IP позволяют указать, какие пакеты IP разрешено передавать во внутреннюю сеть и из нее. Защита сети основана на фильтрации пакетов в соответствии с заданными правилами. Функция NAT позволяет скрыть незарегистрированные частные IP-адреса за набором зарегистрированных IP-адресов. Таким образом, она защищает внутреннюю сеть от пользователей внешних сетей. Кроме того, NAT частично решает проблему истощения запаса IP-адресов, так как она позволяет представить большое количество частных адресов с помощью нескольких зарегистрированных адресов. Более подробную информацию можно найти в справочной системе iSeries Information Center.

Сервер Proxy HTTP

Сервер Proxy HTTP поставляется вместе с продуктом IBM HTTP Server for iSeries. HTTP Server является компонентом OS/400. Сервер Proxy принимает запросы HTTP от Web-браузеров и отправляет их Web-серверам. Web-серверам, принимающим запросы, известен только IP-адрес сервера Proxy. Они не могут определить имена или адреса компьютеров, отправивших запрос. Сервер Proxy может обрабатывать запросы к HTTP, FTP, Gopher и WAIS.

Все Web-страницы, возвращаемые в ответ на запросы пользователей сервера Proxy, помещаются в кэш этого сервера. Таким образом, при получении запроса на страницу сервер Proxy пытается найти ее в кэше. Если нужная страница найдена, она возвращается пользователю. Кэширование страниц позволяет серверу Proxy сократить время поиска Web-страниц и уменьшить число запросов к Web-серверу.

Кроме того, сервер Proxy может отслеживать и заносить в протокол все запросы с URL. Это позволяет вести контроль за использованием сетевых ресурсов.

Поддержка Proxy HTTP в IBM HTTP Server может использоваться для настройки централизованного доступа к Web-ресурсам. Адреса клиентов PC скрыты от Web-серверов, обрабатывающих запросы; им известен лишь IP-адрес сервера Proxy. Кэширование Web-страниц позволяет понизить требования к пропускной способности линии связи и уменьшить нагрузку на брандмауэр. Дополнительная информация приведена на домашней странице IBM HTTP Server for iSeries: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Виртуальная частная сеть (VPN)

Виртуальная частная сеть (VPN) позволяет расширить внутреннюю сеть организации за счет общей сети, например, Internet, сохранив высокий уровень защиты сети. VPN управляет передачей данных по сети и предоставляет такие базовые функции защиты, как идентификация и обеспечение конфиденциальности данных.

Функция VPN OS/400 - это дополнительный компонент программы Навигатор iSeries, графического пользовательского интерфейса (GUI) для OS/400. Эта функция позволяет создать защищенное соединение между двумя конечными точками, в роли которых может выступать хост или шлюз. Для защиты данных, передаваемых по соединению, в VPN OS/400 применяются функции идентификации, шифрования и другие средства.

В стеке протоколов TCP/IP VPN находится на сетевом уровне. В частности, VPN применяет открытую Архитектуру защиты IP (IPSec). IPSec предоставляет основные функции защиты в сети Internet, а также различные компоненты, на основе которых можно создать надежную, защищенную виртуальную частную сеть.

Кроме того, VPN поддерживает протокол L2TP. Соединения L2TP, или виртуальные линии, предоставляют недорогой способ подключения для удаленных пользователей. IP-адреса таким пользователям предоставляет корпоративный сервер. Для защиты соединений L2TP, устанавливаемых с системой или внутренней сетью, может применяться IPSec.

Важно понимать, что VPN повлияет на работу всей сети. В связи с этим требуется тщательно спланировать конфигурацию VPN и не допустить ошибок при ее реализации. Перед настройкой VPN ознакомьтесь с описанием этой функции, приведенным в соответствующем разделе iSeries Information Center. За дополнительной информацией обратитесь к разделу iSeries Information Center—>Защита—>Виртуальная частная сеть. Информация о работе со справочной системой iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Secure Sockets Layer (SSL)

Протокол Secure Sockets Layer (SSL) - это стандартный протокол, применяемый приложениями для настройки защищенных соединений через незащищенную сеть, например, Internet. Этот протокол позволяет установить соединение между приложениями клиента и сервера с идентификацией одной или обеих конечных точек соединения. Кроме того, SSL обеспечивает конфиденциальность и целостность данных, которыми обмениваются клиент и сервер. Дополнительная информация приведена в разделе iSeries Information Center–>Защита—>Secure Sockets Layer (SSL). Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Рекомендации по защите среды TCP/IP

В этом разделе приведены общие советы по организации защиты среды TCP/IP вашей системы. Эти советы касаются общей конфигурации TCP/IP, а не конкретных приложений. Конкретные приложения обсуждаются в следующих разделах.

- Приложение TCP/IP, подключенное к порту, должно быть надежно защищено. Его необходимо создавать с учетом того, что кто-то может попытаться использовать его для несанкционированного доступа. В частности, возможны попытки подключиться к нему с помощью TELNET.
- Отслеживайте использование портов TCP/IP вашей системы. Пользовательское приложение, подключенное к порту TCP/IP, может входить в вашу систему “через черный ход”, т.е. без идентификации. Пользовательское приложение может быть подключено к порту TCP или UDP пользователем с достаточными правами доступа.
- Администратор защиты должен знать о технике *перехвата IP-адресов*, применяемой для несанкционированного доступа. Каждой системе в сети TCP/IP присвоен некоторый IP-адрес. Перехватом IP-адреса называется ситуация, когда третья сторона выдает себя за систему с IP-адресом, которому вы доверяете. Например, это может быть IP-адрес системы, с которой вы обычно устанавливаете соединение.

  Перехват IP-адреса возможен в незащищенной сети, включающей коммутируемые соединения или динамическую маршрутизацию. Для защиты от перехвата IP-адреса выполните приведенные здесь рекомендации, касающиеся

идентификации при входе в систему и защиты на уровне объектов. Убедитесь также в том, что в системе правильно выбраны ограничения на объем ASP. Это защитит систему от преднамеренного переполнения ненужной почтой и буферными файлами с целью вывода ее из строя.

Кроме того, отслеживайте работу TCP/IP. При обнаружении перехвата IP-адреса найдите слабые места в защите TCP/IP и постарайтесь их устранить.

- Во внутренней сети Intranet (сети IP, действующей независимо от Internet) используйте специально выделенные для этого IP-адреса. Пакеты с такими адресами не будут передаваться в сети Internet. Таким образом, внутренние адреса обеспечивают дополнительный уровень защиты вашей сети.

  Дополнительную информацию о присвоении IP-адресов, диапазонах IP-адресов и защите соединений TCP/IP можно найти в разделе iSeries Information Center—>Сеть—>TCP/IP.
- Если вы планируете подключить систему к Internet или внутренней сети, ознакомьтесь с рекомендациями по защите, приведенными в документе *SecureWay: iSeries и Internet* (iSeries Information Center—>Защита—>SecureWay). Информация о работе со справочной системой iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Управление автоматическим запуском серверов TCP/IP

Администратор защиты должен выбрать серверы TCP/IP, которые будут запускаться автоматически вместе с подсистемой TCP/IP. Подсистема TCP/IP может быть запущена двумя различными командами, при этом автоматически запускаемые серверы определяются по-разному.

Эти две команды, а также советы по организации защиты приведены в Табл. 22. Параметры автоматического запуска по умолчанию приведены в Табл. 23 на стр. 129. Эти параметры можно изменить командами CHGxxxA (Изменить атрибуты xxx) сервера. Например, параметры сервера TELNET изменяются командой CHGTELNA.

Таблица 22. Серверы, запускаемые различными командами TCP/IP

Команда	Запускаемые серверы	Рекомендации по защите
Запустить TCP/IP (STRTCP)	Будет запущен каждый сервер с параметром AUTOSTART(*YES). Значения этого параметра по умолчанию приведены в Табл. 23 на стр. 129.	• Права доступа *IOSYSCFG должны быть предоставлены только тем пользователям, которым вы доверяете настройку автоматического запуска серверов TCP/IP. • Настройка прав доступа к команде STRTCP существенно влияет на защиту. По умолчанию общие права доступа к этой команде равны *EXCLUDE. • Настройте контроль для команд Изменить атрибуты *сервера* (таких как CHGTELNA) и отслеживайте все попытки изменить значение параметра AUTOSTART.

Таблица 22. Серверы, запускаемые различными командами TCP/IP (продолжение)

Команда	Запускаемые серверы	Рекомендации по защите
Запустить сервер TCP/IP (STRTCPSVR)	Запускаемые серверы указываются в параметре этой команды. По умолчанию запускаются все серверы.	• Командой Изменить значения по умолчанию команды (CHGCMDDFT) вы можете настроить команду STRTCPSVR на запуск только одного из серверов. Это не помешает пользователям с соответствующими правами доступа запустить другие серверы. Однако это сделает случайный запуск всех серверов менее вероятным. Например, для того чтобы по умолчанию запускался только сервер TELNET, введите следующую команду: `CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **Примечание:** При изменении значения по умолчанию можно указать только один сервер. Выберите либо постоянно используемый, либо наименее опасный с точки зрения защиты (такой как TFTP) сервер. • Настройка прав доступа к команде STRTCPSVR существенно влияет на защиту. По умолчанию общие права доступа к этой команде равны *EXCLUDE.

В приведенной ниже таблице указаны значения параметра автоматического запуска, заданные для серверов TCP/IP. Дополнительная информация об этих серверах приведена в справочной системе iSeries Information Center (**Сеть—>TCP/IP**). Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Таблица 23. Значение по умолчанию для параметра автоматического запуска серверов TCP/IP

Сервер	Значение по умолчанию	Ваше значение
TELNET	AUTOSTART(*YES)	
FTP (Протокол передачи файлов)	AUTOSTART(*YES)	
BOOTP (Протокол начальной загрузки)	AUTOSTART(*NO)	
TFTP (Упрощенный протокол передачи файлов)	AUTOSTART(*NO)	
REXEC (Сервер удаленного выполнения)	AUTOSTART(*NO)	
RouteD (Демон маршрутизации)	AUTOSTART(*NO)	
SMTP (Простой протокол передачи почты)	AUTOSTART(*YES)	
POP (Почтовый протокол)	AUTOSTART(*NO)	
HTTP (Протокол передачи гипертекстовой информации)[1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (Демон построчной печати)	AUTOSTART(*YES)	
SNMP (Простой протокол управления сетью)	AUTOSTART(*YES)	
DNS (Система имен доменов)	AUTOSTART(*NO)	
DDM (Управление распределенными данными)	AUTOSTART(*NO)	
DHCP (Протокол динамической настройки хостов)	AUTOSTART(*NO)	

Таблица 23. Значение по умолчанию для параметра автоматического запуска серверов TCP/IP (продолжение)

Сервер	Значение по умолчанию	Ваше значение
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Примечания:

1. Для настройки параметра AUTOSTART сервера IBM HTTP Server for iSeries применяется команда CHGHTTPA.

Рекомендации по защите соединений SLIP

Функции TCP/IP сервера iSeries включают в себя Протокол подключения к Internet по последовательной линии (SLIP). Этот протокол позволяет создавать простые двухточечные соединения. Пользователь SLIP может подключаться к локальной или глобальной сети, создавая двухточечное соединение с системой, находящейся в этой сети.

Протокол SLIP работает с асинхронными соединениями. Он может применяться для настройки входящих и исходящих коммутируемых соединений с сервером iSeries. Например, SLIP может применяться при вызове системы iSeries из персонального компьютера. После установления соединения SLIP вы можете подключить клиент TELNET на PC к серверу TELNET в системе iSeries, а также передавать файлы между двумя системами по протоколу FTP.

Первоначально в системе отсутствует конфигурация SLIP. По этой причине, если вы не собираетесь работать со SLIP (или с TCP/IP по коммутируемым соединениям), не создавайте профайлы конфигурации SLIP. Конфигурации SLIP создаются командой Работа с двухточечным TCP/IP (WRKTCPPTP). Для работы с командой WRKTCPPTP нужны специальные права доступа *IOSYSCFG.

Для работы со SLIP необходимо создать один или несколько профайлов конфигурации SLIP. Профайлы конфигурации могут работать в одном из следующих режимов:

- Входящее соединение (*ANS)
- Исходящее соединение (*DIAL)

В следующих разделах обсуждается настройка защиты в профайлах конфигурации SLIP.

Примечание: **Пользовательский профайл** - это объект сервера iSeries, необходимый для входа пользователя в систему. Каждое задание сервера iSeries работает под управлением некоторого пользовательского профайла. В **профайле конфигурации** хранится информация, применяемая для установления соединения SLIP с системой iSeries. При установлении соединения SLIP с сервером iSeries создается только канал связи. При этом пользователь не входит в систему, а на сервере iSeries не запускается задание. Следовательно, для установления соединения SLIP с сервером iSeries пользовательский профайл не нужен. Однако, как будет ясно из дальнейшего, профайлу конфигурации SLIP может потребоваться пользовательский профайл, чтобы разрешить или запретить соединение.

Управление входящими соединениями SLIP

Для того чтобы удаленные системы могли устанавливать соединения SLIP с системой AS/400, необходимо создать профайл конфигурации SLIP типа *ANS. Для создания или изменения профайла конфигурации SLIP служит команда Работа с двухточечным TCP/IP (WRKTCPPTP). Активизировать профайл конфигурации можно с помощью команды Запустить двухточечный TCP/IP (STRTCPPTP) или опции меню WRKTCPPTP. Первоначально с командами STRTCPPTP и ENDTCPPTP связаны общие права доступа *EXCLUDE. Опции добавления, изменения и удаления профайлов конфигурации SLIP доступны, только если у вас есть специальные права доступа *IOSYSCFG. Для управления доступом к этим командам администратор защиты может настраивать права доступа к командам и специальные права доступа пользователей.

Защита входящих соединений SLIP

При идентификации удаленных систем, пытающихся установить соединение, локальная система запрашивает у них идентификатор и пароль пользователя. Затем локальная система проверяет полученную информацию. Если идентификатор и пароль указаны неправильно, запрос на соединение отклоняется.

Для настройки процедуры идентификации входящих соединений выполните следующие действия:

__ Шаг 1. Создайте пользовательский профайл, который будет применяться удаленной системой для установления соединения. Запрашивающая система должна будет передать идентификатор и пароль этого профайла.

Примечание: Для того чтобы система действительно выполняла проверку паролей, системное значение QSECURITY должно быть не меньше 20.

В качестве дополнительной меры по защите системы рекомендуется создавать для соединений SLIP специальные пользовательские профайлы с ограниченными правами доступа. Если пользовательский профайл применяется только для установления соединения SLIP, укажите в нем следующие значения:

- Начальное меню (INLMNU): *SIGNOFF
- Начальная программа (INLPGM): *NONE.
- Ограничить возможности (LMTCPB): *YES

Указанные значения предотвратят вход пользователей в систему под управлением этого пользовательского профайла.

__ Шаг 2. Создайте список прав доступа, который будет проверяться системой при поступлении запроса на установление соединения SLIP.

Примечание: Этот список прав доступа должен быть указан в поле *Системный список прав доступа* профайла SLIP. (См. шаг 4.)

__ Шаг 3. Командой Добавить запись списка прав доступа (ADDAUTLE) добавьте пользователя, созданного на шаге 1, в список прав доступа. Вы можете создать свой список прав доступа для каждого профайла конфигурации SLIP или использовать один список прав доступа с несколькими профайлами.

__ Шаг 4. Командой WRKTCPPTP создайте профайл SLIP типа *ANS со следующими характеристиками:

- Профайл конфигурации должен применять сценарий установления соединения, включающий идентификацию пользователя, т.е. получение идентификатора и пароля пользователя от запрашивающей системы и их проверку. Несколько таких сценариев поставляются с системой.

- В профайле конфигурации должно быть указано имя списка прав доступа, созданного на шаге 2. В этом списке должен присутствовать идентификатор пользователя, ожидаемый сценарием установления соединения.

Учтите, что эффективность защиты входящих соединений зависит от возможностей защиты вызывающей системы. Идентификатор и пароль пользователя передаются сценарием вызывающей системы. В некоторых системах, таких как iSeries, имена и пароли пользователей хранятся в защищенном виде. (Способ защиты описан в разделе “Защита исходящих соединений”.) В других системах идентификатор и пароль, указанные в сценарии, доступны любому, кто знает о местонахождении сценария.

В силу вышесказанного, рекомендуется создавать различные профайлы конфигурации для разных запрашивающих систем. В команде STRTCPPTP настройте прием соединений для конкретного профайла конфигурации. Например, для некоторого профайла конфигурации вы можете разрешить установление соединений только в определенное время суток. Кроме того, рекомендуется настроить контроль за действиями для отслеживания операций, выполняемых в соединении.

Предотвращение входа удаленных пользователей в другие системы

При некоторых конфигурациях системы и локальной сети пользователь, установивший соединение SLIP, может получить доступ к другим системам сети, не входя в ту систему, с которой он установил соединение. Например, если пользователь установил соединение SLIP с одной из систем локальной сети, он может установить соединение FTP с другой системой этой сети, даже если соединения SLIP с ней запрещены.

Для того чтобы пользователь SLIP не мог устанавливать соединения с другими системами вашей сети, укажите N (Нет) в параметре *Разрешить пересылку IP-дейтаграмм* профайла конфигурации. Это не позволит пользователю получать доступ к вашей сети до входа в систему. Однако после входа в систему параметр Разрешить пересылку IP-дейтаграмм не действует. В частности, он не ограничивает доступ пользователя к приложениям TCP/IP системы iSeries (таким как FTP и TELNET), позволяющим устанавливать соединения с другими системами сети.

Управление исходящими соединениями

Для установления исходящих соединений SLIP в системе необходимо создать профайл конфигурации SLIP типа *DIAL. Для создания или изменения профайла конфигурации SLIP служит команда Работа с двухточечным TCP/IP (WRKTCPPTP). Активизировать профайл конфигурации можно с помощью команды Запустить двухточечный TCP/IP (STRTCPPTP) или опции меню WRKTCPPTP. Первоначально с командами STRTCPPTP и ENDTCPPTP связаны общие права доступа *EXCLUDE. Опции добавления, изменения и удаления профайлов конфигурации SLIP доступны, только если у вас есть специальные права доступа *IOSYSCFG. Для управления доступом к этим командам администратор защиты может настраивать права доступа к командам и специальные права доступа пользователей.

Защита исходящих соединений

Пользователям системы iSeries может потребоваться установление соединений SLIP с удаленными системами, требующими идентификации. В этом случае сценарий установления соединения сервера iSeries должен передавать в удаленную систему идентификатор и пароль пользователя. На сервере iSeries пароли хранятся в зашифрованном виде. Пароль не обязательно должен храниться в сценарии установления соединения.

Примечания:

1. Хотя система и хранит пароль соединения в зашифрованном виде, перед отправкой он расшифровывается. Пароли SLIP, как и пароли FTP и TELNET, передаются в незашифрованном виде (“как есть”). Однако, в отличие от паролей FTP и TELNET, пароль SLIP передается до установления соединения TCP/IP.

   Поскольку SLIP работает с двухточечным соединением в асинхронном режиме, риск нарушения защиты при передаче незашифрованных паролей определяется иными факторами, нежели в случае протоколов FTP и TELNET. Незашифрованные пароли FTP и TELNET передаются по сети в виде IP-данных и уязвимы к перехвату IP-адреса. Защищенность же пароля SLIP определяется надежностью телефонного соединения между двумя системами.
2. По умолчанию сценарии установления соединения SLIP хранятся в файле QUSRSYS/QATOCPPSCR. Общие права доступа к этому файлу по умолчанию равны *USE, что запрещает обычным пользователям изменять сценарии.

При создании профайла соединения с удаленной системой, требующей идентификации, выполните следующие действия:

__ Шаг 1. Убедитесь в том, что системное значение Сохранить идентификационные данные на сервере (QRETSVRSEC) равно 1 (Да). Это системное значение определяет, должны ли пароли, которые могут быть расшифрованы, храниться в защищенной области системы.

__ Шаг 2. Командой WRKTCPPTP создайте профайл конфигурации SLIP со следующими характеристиками:

- В качестве режима профайла конфигурации укажите *DIAL.
- В параметре *Имя доступа к удаленной службе* укажите идентификатор пользователя, ожидаемый удаленной системой. Например, при подключении к другому серверу iSeries укажите имя пользовательского профайла этого сервера.
- В параметре *Пароль доступа к удаленной службе* укажите пароль, ожидаемый удаленной системой для данного идентификатора. На сервере iSeries этот пароль хранится в защищенной области в зашифрованном виде. Имена и пароли, указанные в профайлах конфигурации, связаны с пользовательским профайлом QTCP. Эти имена и пароли недоступны для пользовательских команд и интерфейсов. Они доступны только для зарегистрированных системных программ.

  Примечание: Учтите, что пароли профайлов конфигурации не сохраняются с файлами конфигурации TCP/IP. Для сохранения паролей SLIP сохраните пользовательский профайл QTCP командой Сохранить данные о защите (SAVSECDTA).
- Укажите сценарий установления соединения, передающий идентификатор и пароль пользователя. Несколько таких сценариев поставляются с системой. При запуске сценария система расшифровывает пароль и передает его удаленной системе.

Рекомендации по защите двухточечных соединений

Двухточечный протокол (PPP) входит в состав TCP/IP. PPP - это промышленный стандарт двухточечных соединений, предоставляющий дополнительные возможности по сравнению со SLIP.

PPP позволяет серверу iSeries устанавливать высокоскоростные соединения с провайдером Internet и другими системами во внутренней и внешней сети. Кроме того, сервер iSeries можно подключить к удаленным локальным сетям с помощью коммутируемых соединений.

PPP, как и SLIP, создает сетевое соединение с сервером iSeries. Соединение PPP не осуществляет вход в систему, а лишь создает канал связи. После установления соединения PPP для входа в систему и подключения к серверам TCP/IP, таким как TELNET и FTP, по-прежнему требуется указать идентификатор и пароль пользователя. Ниже приведена информация о защите в соединениях PPP:

Примечание: Если на рабочей станции установлен продукт IBM iSeries Access для Windows, для настройки PPP можно воспользоваться программой Навигатор.

- PPP позволяет создавать выделенные соединения (в которых пользователю всегда присвоен один IP-адрес). Это делает систему уязвимой к перехвату IP-адреса (при котором третья система выдает себя за данную, зная этот IP-адрес). Для защиты от перехвата IP-адреса в протоколе PPP расширены возможности идентификации.
- Для PPP, как и для SLIP, необходимо создать профайл соединения с именем и паролем пользователя. Однако, в отличие от SLIP, пользователю не обязательно иметь в системе iSeries пользовательский профайл. Имя пользователя и пароль профайла соединения PPP могут быть не связаны ни с одним из пользовательских профайлов системы iSeries. Вместо этого для идентификации PPP применяются контрольные списки. Кроме того, PPP не требует сценария установления соединения. Идентификация (передача и проверка имени пользователя и пароля) интегрирована в архитектуру PPP и происходит на более низком уровне, чем в SLIP.
- С PPP может применяться протокол CHAP (протокол идентификации с квитированием связи по вызову). Вы можете больше не беспокоиться о подслушивании и перехвате паролей, поскольку CHAP шифрует имена и пароли пользователей.

  CHAP будет применяться при установлении соединения PPP, только если обе стороны поддерживают этот протокол. Согласование протоколов идентификации выполняется при установлении соединения. Например, если система A поддерживает CHAP, а система B - нет, то система A может либо отклонить запрос на соединение, либо согласиться работать с незашифрованным именем и паролем пользователя. Последнее называется снижением защиты. Снижение защиты - это настраиваемая опция. В сети Intranet, если известно, что все системы поддерживают CHAP, рекомендуется запретить снижение защиты. При установлении внешних соединений может потребоваться разрешить снижение защиты для некоторых удаленных систем.

  Профайл соединения PPP позволяет указать допустимые IP-адреса. Например, вы можете указать, что данному пользователю должен быть предоставлен конкретный IP-адрес или IP-адрес из некоторого диапазона. Эта возможность, вместе с шифрованием паролей, усиливает защиту от перехвата адреса.

  В качестве дополнительной защиты от перехвата IP-адреса и перехвата активного сеанса можно настроить в PPP повторную идентификацию через заданный интервал времени. Например, пока сеанс PPP активен, сервер iSeries может повторно запросить имя и пароль пользователя у удаленной системы. Для того чтобы быть уверенной, что удаленная система не изменилась, система AS/400 повторяет такой запрос каждые 15 минут. (Это никак не отразится на работе конечных пользователей. Системы обмениваются именами и паролями пользователей на более низком уровне.)

PPP позволяет удаленным локальным сетям подключаться к серверу iSeries и его локальной сети по коммутируемым линиям связи. В этом случае, как правило, необходима поддержка пересылки IP-дейтаграмм. Пересылка IP-дейтаграмм позволяет удаленным системам получать доступ не только к вашей системе, но и к локальной сети, что может представлять опасность для защиты. Однако PPP обладает соответствующими средствами защиты (такими как шифрование паролей и проверка IP-адресов). Это снижает вероятность взлома вашей сети через коммутируемое соединение PPP.

Дополнительная информация о PPP приведена в справочной системе iSeries Information Center.

Рекомендации по защите сервера Протокола начальной загрузки

Протокол начальной загрузки (BOOTP) позволяет динамически связывать рабочие станции с серверами, назначать им IP-адреса и выбирать источники IPL (загрузки начальной программы).

Протокол BOOTP - это протокол из семейства TCP/IP, который позволяет бездисковым рабочим станциям (клиентам) загружать с сервера файл с начальным кодом. Стандартный порт сервера BOOTP - 67. Когда сервер получает запрос от клиента, он находит IP-адрес клиента и возвращает ему файл, содержащий этот IP-адрес и имя загрузочного файла. После этого клиент отправляет серверу запрос TFTP на получение загрузочного файла. Таблица соответствия аппаратных адресов клиентов и IP-адресов хранится на сервере iSeries.

Ограничение доступа к BOOTP

Если вы не применяете клиенты, которые загружаются по сети, то сервер BOOTP не нужно запускать в системе. Он может применяться и для поддержки других устройств, однако в этом случае вместо него лучше применять сервер DHCP. Для того чтобы запретить запуск сервера BOOTP, выполните следующие действия:

__ Шаг 1. Отключите автоматический запуск заданий сервера BOOTP при запуске TCP/IP командой:

```
CHGBPA AUTOSTART(*NO)
```

Примечания:

a. AUTOSTART(*NO) - это значение по умолчанию.

b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

__ Шаг 2. Для того чтобы запретить подключение пользовательских приложений, в частности, приложений с API сокетов, к порту, обычно занятому BOOTP, выполните следующие действия:

Примечание: Поскольку серверы DHCP и BOOTP применяют один и тот же порт, после выполнения описанной процедуры серверу DHCP также будет запрещено использовать этот порт. Не ограничивайте доступ к порту, если вы планируете применять DHCP.

__ Шаг a. Введите `GO CFGTCP`. Будет показано меню Настроить TCP/IP.

__ Шаг b. Выберите опцию 4 (Работа с ограничениями на порты TCP/IP).

__ Шаг c. В меню Работа с ограничениями на порты TCP/IP выберите опцию 1 (Добавить).

__ Шаг d. В качестве нижней границы диапазона портов укажите `67`.

__ Шаг e. В качестве верхней границы диапазона портов укажите *ONLY.

Примечания:

1) Ограничение на использование порта вступит в силу при следующем запуске TCP/IP. Если во время настройки ограничений на использование порта протокол TCP/IP активен, перезапустите его.
2) Информация о назначении общих номеров портов приведена в RFC1700.

__ Шаг f. В параметре Протокол укажите *UDP.

__ Шаг g. В поле Пользовательский профайл укажите имя защищенного профайла, определенного в системе. (Защищенным называется пользовательский профайл, которому не принадлежат никакие программы, принимающие права доступа, и пароль которого не известен другим пользователям.) Выделяя порт конкретному пользователю, вы автоматически запрещаете его применение всем остальным пользователям.

Защита сервера BOOTP

Сервер BOOTP не предоставляет доступ к системе iSeries, поэтому его применение не может серьезно угрожать безопасности системы. Основная задача администратора защиты состоит в проверке правильности IP-адресов, связанных с клиентами, загружающимися по сети. Злоумышленник может изменить таблицу BOOTP, указав неправильный адрес клиента или удалив запись об этом клиенте.

Для работы с сервером BOOTP и таблицей BOOTP необходимы специальные права доступа *IOSYSCFG. Убедитесь, что права доступа *IOSYSCFG предоставлены лишь тем пользовательским профайлам, которым они действительно необходимы.

Рекомендации по защите сервера DHCP

Протокол динамической настройки хостов (DHCP) применяется для передачи информации о конфигурации хостам сети TCP/IP. В случае клиентских рабочих станций DHCP выполняет функции автоматической настройки. Программа клиентской рабочей станции, поддерживающая DHCP, рассылает запросы на информацию о конфигурации методом оповещения. Если в системе iSeries запущен сервер DHCP, он отвечает на запрос, отправляя клиентской рабочей станции информацию о конфигурации TCP/IP.

Протокол DHCP упрощает процедуру первого подключения к серверу iSeries. Если запущен сервер DHCP, пользователям не нужно вводить информацию о конфигурации TCP/IP. Кроме того, протокол DHCP позволяет сократить число внутренних IP-адресов, необходимых в подсети. Сервер DHCP может временно выделять IP-адреса из пула адресов активным пользователям.

При работе с клиентами, загружающимися по сети, протокол DHCP может применяться вместо протокола BOOTP. По сравнению с BOOTP, DHCP предоставляет более широкий набор функций. Кроме того, он поддерживает динамическую настройку как клиентов, загружающихся по сети, так и PC.

Ограничение доступа к системе через DHCP

Для того чтобы *полностью запретить* доступ к системе через DHCP, выполните следующие действия:

1. Отключите автоматический запуск заданий сервера DHCP при запуске TCP/IP командой:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Примечания:

   a. AUTOSTART(*NO) - это значение по умолчанию.

   b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

2. Для того чтобы запретить подключение пользовательских приложений, в частности, приложений с API сокетов, к порту, обычно занятому DHCP, выполните следующие действия:

   a. Введите `GO CFGTCP`. Будет показано меню Настроить TCP/IP.

   b. Выберите опцию 4 (Работа с ограничениями на порты TCP/IP).

   c. В меню Работа с ограничениями на порты TCP/IP выберите опцию 1 (Добавить).

   d. В качестве нижней границы диапазона портов укажите `67`.

   e. В качестве верхней границы диапазона портов укажите `68`.

      Примечания:

      1) Ограничение на использование порта вступит в силу при следующем запуске TCP/IP. Если во время настройки ограничений на использование порта протокол TCP/IP активен, перезапустите его.

      2) Информация о назначении общих номеров портов приведена в RFC1700.

   f. В параметре Протокол укажите `*UDP`.

   g. В поле Пользовательский профайл укажите имя защищенного профайла, определенного в системе. (Защищенным называется пользовательский профайл, которому не принадлежат никакие программы, принимающие права доступа, и пароль которого не известен другим пользователям.) Выделяя порт конкретному пользователю, вы автоматически запрещаете его применение всем остальным пользователям.

Защита сервера DHCP

Ниже приведена информация о сервере DHCP:

- Ограничьте число пользователей, у которых есть права на администрирование сервера DHCP. Для администрирования сервера DHCP необходимы следующие права доступа:
  - Специальные права доступа *IOSYSCFG
  - Права доступа *RW к следующим файлам:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```

- Оцените, насколько физически защищена ваша локальная сеть. Возможно ли проникнуть в ваше помещение с портативным компьютером и физически подключить его к локальной сети? Если да, то вы можете создать список клиентов (их аппаратных адресов), которых будет обслуживать сервер DHCP. Это приведет к некоторому снижению эффективности работы сервера DHCP, зато система не будет настраивать неизвестные рабочие станции.
- Рекомендуется применять пул локальных IP-адресов, неизвестных в Internet. В этом случае рабочие станции из внешней сети не смогут получить информацию о конфигурации от сервера.

- Точки выхода DHCP позволяют реализовать дополнительные функции защиты. Ниже приведено описание точек выхода и их функций. Информацию о работе с этими точками выхода см. в книге *iSeries System API Reference*.

  Запись в порт
  Система вызывает программу выхода при чтении пакета данных из порта 67 (порта DHCP). Программе выхода передается весь пакет данных. Эта программа может решить, должна ли система обрабатывать пакет. Точка выхода может применяться в случае, когда встроенных защитных функций DHCP недостаточно.

  Присвоение адреса
  Система вызывает программу выхода каждый раз, когда сервер DHCP формально присваивает адрес клиенту.

  Освобождение адреса
  Система вызывает программу выхода каждый раз, когда сервер DHCP освобождает адрес и помещает его обратно в пул адресов.

Рекомендации по защите сервера TFTP

Упрощенный протокол передачи файлов (TFTP) предоставляет основные функции по передаче файлов без идентификации пользователей. Протокол TFTP работает совместно с протоколом начальной загрузки (BOOTP) или протоколом динамической настройки хостов (DHCP).

Сначала клиент подключается к серверу BOOTP или DHCP. Сервер BOOTP или сервер DHCP отправляют ответ, содержащий IP-адрес клиента и имя загрузочного файла. После этого клиент отправляет серверу запрос TFTP на получение загрузочного файла. После получения загрузочного файла клиент закрывает сеанс TFTP.

Ограничение доступа через TFTP

Если вы не применяете клиенты, которые загружаются по сети, то сервер TFTP не нужно запускать в системе. Для того чтобы запретить запуск сервера TFTP, выполните следующие действия:

__ Шаг 1. Отключите автоматический запуск заданий сервера TFTP при запуске TCP/IP командой:

```
CHGTFTPA AUTOSTART(*NO)
```

Примечания:

a. AUTOSTART(*NO) - это значение по умолчанию.

b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

__ Шаг 2. Для того чтобы запретить подключение пользовательских приложений, в частности, приложений с API сокетов, к порту, обычно занятому TFTP, выполните следующие действия:

__ Шаг a. Введите `GO CFGTCP`. Будет показано меню Настроить TCP/IP.

__ Шаг b. Выберите опцию 4 (Работа с ограничениями на порты TCP/IP).

__ Шаг c. В меню Работа с ограничениями на порты TCP/IP выберите опцию 1 (Добавить).

__ Шаг d. В качестве нижней границы диапазона портов укажите `69`.

__ Шаг e. В качестве верхней границы диапазона портов укажите `*ONLY`.

Примечания:

1) Ограничение на использование порта вступит в силу при следующем запуске TCP/IP. Если во время настройки ограничений на использование порта протокол TCP/IP активен, перезапустите его.
2) Информация о назначении общих номеров портов приведена в RFC1700.

__ Шаг f. В параметре Протокол укажите *UDP*.

__ Шаг g. В поле Пользовательский профайл укажите имя защищенного профайла, определенного в системе. (Защищенным называется пользовательский профайл, которому не принадлежат никакие программы, принимающие права доступа, и пароль которого не известен другим пользователям.) Выделяя порт конкретному пользователю, вы автоматически запрещаете его применение всем остальным пользователям.

Защита сервера TFTP

По умолчанию сервер TFTP предоставляет крайне ограниченный доступ к системе iSeries. Он специально предназначен для передачи исходного кода клиентам, загружающимся по сети. Администратор защиты должен знать о следующих особенностях сервера TFTP:

- Сервер TFTP не выполняет идентификацию (не запрашивает ИД пользователя и пароль). Все задания TFTP выполняются под управлением пользовательского профайла QTFTP. С этим профайлом не связан пароль. Следовательно, он не может применяться для входа в систему в интерактивном режиме. У пользовательского профайла QTFTP нет ни специальных прав доступа, ни прав доступа к ресурсам системы. Для обращения к ресурсам, необходимым для клиентов, загружающихся по сети, этот профайл применяет общие права доступа.
- По умолчанию сервер TFTP настроен для работы с каталогом, содержащим информацию о клиентах, загружающихся по сети. Для чтения и записи данных в этот каталог у вас должны быть права доступа *PUBLIC или права доступа профайла QTFTP. Для записи данных в каталог вам должны быть предоставлены права *CREATE с помощью параметра ″Разрешить запись в файлы″ команды CHGTFTPA. Для записи в существующий файл вам должны быть предоставлены права *REPLACE с помощью того же параметра и команды. Права доступа *CREATE позволяют изменять содержимое существующих файлов и создавать новые файлы. Права доступа *REPLACE позволяют только изменять содержимое существующих файлов.

  Клиенту TFTP запрещен доступ ко всем остальным каталогам, до тех пор пока вы явно не предоставите ему доступ к дополнительным каталогам с помощью команды Изменить атрибуты TFTP (CHGTFTPA). Следовательно, если локальный или удаленный пользователь запустит сеанс TFTP в системе, его возможности получить информацию или нанести ущерб будут в значительной степени ограничены.
- Если помимо поддержки клиентов, загружающихся по сети, сервер TFTP планируется применять для других целей, рекомендуется создать программу выхода, которая будет проверять и идентифицировать запросы TFTP. Сервер TFTP предоставляет такую же точку выхода для проверки запроса, как и сервер FTP. Дополнительная информация приведена в разделе iSeries Information Center—>Сеть—>TCP/IP—>TFTP. Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Рекомендации по защите для сервера REXEC

Сервер удаленного выполнения (REXEC) запускает команды, полученные от клиента REXEC. Обычно в роли клиента REXEC выступает приложение PC или UNIX, поддерживающее отправку команд REXEC. Функции, выполняемые этим сервером, аналогичны функциям команды RCMD (Удаленная команда) сервера FTP.

Ограничение доступа к серверу через REXEC

Если вы не хотите, чтобы сервер iSeries принимал команды от клиентов REXEC, запретите запуск сервера REXEC, выполнив следующие действия:

__ Шаг 1. Отключите автоматический запуск заданий сервера REXEC при запуске TCP/IP командой:

```
CHGRXCA AUTOSTART(*NO)
```

Примечания:

a. AUTOSTART(*NO) - это значение по умолчанию.

b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

__ Шаг 2. Для того чтобы запретить подключение пользовательских приложений, в частности, приложений с API сокетов, к порту, обычно занятому REXEC, выполните следующие действия:

__ Шаг a. Введите `GO CFGTCP`. Будет показано меню Настроить TCP/IP.

__ Шаг b. Выберите опцию 4 (Работа с ограничениями на порты TCP/IP).

__ Шаг c. В меню Работа с ограничениями на порты TCP/IP выберите опцию 1 (Добавить).

__ Шаг d. В качестве нижней границы диапазона портов укажите `512`.

__ Шаг e. В качестве верхней границы диапазона портов укажите `*ONLY`.

__ Шаг f. В качестве протокола укажите `*TCP`.

__ Шаг g. В поле Пользовательский профайл укажите имя защищенного профайла, определенного в системе. (Защищенным называется пользовательский профайл, которому не принадлежат никакие программы, принимающие права доступа, и пароль которого не известен другим пользователям.) Выделяя порт конкретному пользователю, вы автоматически запрещаете его применение всем остальным пользователям.

Примечания:

a. Ограничение на использование порта вступит в силу при следующем запуске TCP/IP. Если во время настройки ограничений на использование порта протокол TCP/IP активен, перезапустите его.

b. Информация о назначении общих номеров портов приведена в RFC1700.

Защита сервера REXEC

Ниже приведена информация о сервере удаленного выполнения:

- Запрос REXCD содержит ИД пользователя, пароль и команду, которую нужно выполнить. Для проверки запроса применяется обычная процедура идентификации и проверки прав доступа сервера iSeries:
  - Проверяется правильность пользовательского профайла и пароля.
  - Для пользовательского профайла устанавливается опция *Ограничить возможности* (LMTCPB).

– Проверяется наличие у пользователя прав на выполнение запрошенной команды, а также прав доступа ко всем ресурсам, используемым командой.

- Сервер REXEC предоставляет те же точки выхода, что и сервер FTP. Вы можете написать программу выхода, которая будет проверять команды и разрешать или запрещать их выполнение. За дополнительной информацией обратитесь к разделу iSeries Information Center—>Сеть—>TCP/IP—>REXEC. Информация о работе со справочной системой iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.
- При запуске сервера REXEC помните, что на него не распространяется схема управления доступом через меню. Убедитесь, что пользователям предоставлены права доступа к объектам в соответствии со стратегией защиты ресурсов.

Рекомендации по защите демона RouteD

Сервер демона маршрутизации (RouteD) обеспечивает поддержку Протокола информации о маршрутизации (RIP) на сервере iSeries. RIP - это наиболее распространенный протокол маршрутизации. За маршрутизацию пакетов IP в автономных системах отвечает Протокол внутренних шлюзов, входящий в состав TCP/IP.

Демон RouteD повышает эффективность передачи данных по сети, поскольку позволяет системам в защищенной сети обмениваться текущей информацией о маршрутах. Если в системе запущен демон RouteD, она может получать обновленную информацию о маршрутизации пакетов от других маршрутизаторов. Следовательно, если сервер RouteD не будет защищен, злоумышленники смогут с его помощью перенаправить пакеты в систему, где они будут скопированы или изменены. Ниже приведены рекомендации по организации защиты сервера RouteD:

- На серверах iSeries применяется протокол RIPv1, который не поддерживает идентификацию маршрутизаторов. Этот протокол предназначен только для защищенной сети. Если в одной сети с вашей системой находятся незащищенные системы, не следует запускать сервер RouteD. Для того чтобы отключить автоматический запуск сервера RouteD, выполните следующую команду:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Примечания:

  1. AUTOSTART(*NO) - это значение по умолчанию.
  2. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.
- Убедитесь, что специальные права доступа *IOSYSCFG, позволяющие изменить конфигурацию сервера RouteD, предоставлены лишь тем пользователям, которым они действительно необходимы.
- Если система подключена к нескольким сетям (например, к корпоративной сети и к сети Internet), вы можете настроить сервер RouteD таким образом, чтобы он получал обновления только из защищенной сети.

Рекомендации по защите сервера DNS

Сервер имен доменов (DNS) преобразует имя хоста в IP-адрес и наоборот. В системе iSeries сервер DNS предназначен для преобразования адресов внутренней, защищенной сети (корпоративной сети).

Ограничение доступа к системе через DNS

Для того чтобы *полностью запретить* доступ к системе через DNS, выполните следующие действия:

1. Отключите автоматический запуск заданий сервера DNS при запуске TCP/IP командой:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Примечания:

   a. AUTOSTART(*NO) - это значение по умолчанию.

   b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

2. Для того чтобы запретить подключение пользовательских приложений, в частности, приложений с API сокетов, к порту, обычно занятому DNS, выполните следующие действия:

   a. Введите `GO CFGTCP`. Будет показано меню Настроить TCP/IP.

   b. Выберите опцию 4 (Работа с ограничениями на порты TCP/IP).

   c. В меню Работа с ограничениями на порты TCP/IP выберите опцию 1 (Добавить).

   d. В качестве нижней границы диапазона портов укажите `53`.

   e. В качестве верхней границы диапазона портов укажите `*ONLY`.

      Примечания:

      1) Ограничение на использование порта вступит в силу при следующем запуске TCP/IP. Если во время настройки ограничений на использование порта протокол TCP/IP активен, перезапустите его.

      2) Информация о назначении общих номеров портов приведена в RFC1700.

   f. В качестве протокола укажите `*TCP`.

   g. В поле Пользовательский профайл укажите имя защищенного профайла, определенного в системе. (Защищенным называется пользовательский профайл, которому не принадлежат никакие программы, принимающие права доступа, и пароль которого не известен другим пользователям.) Выделяя порт конкретному пользователю, вы автоматически запрещаете его применение всем остальным пользователям.

   h. Повторите шаги с 2c по 2g для протокола *UDP.

Защита сервера DNS

Ниже приведена информация о сервере DNS:

- Сервер DNS преобразует IP-адреса и имена хостов. Он не предоставляет доступ к объектам системы iSeries. Опасность состоит в том, что получив доступ к серверу DNS, можно легко определить топологию сети. Кроме того, с помощью DNS можно узнать адреса систем, которые могут быть атакованы в будущем. Однако сервер DNS не содержит информации, с помощью которой можно получить доступ к этим системам.
- Обычно сервер DNS системы iSeries применяется только в локальной сети. В связи с этим, доступ к DNS чаще всего не ограничивается. Однако в случае, когда ваша сеть разбита на несколько подсетей, может потребоваться запретить пользователям некоторых подсетей доступ к DNS на сервере iSeries. Одна из функций защиты DNS позволяет ограничить доступ к основному домену. С помощью Навигатора iSeries можно задать IP-адрес системы, которой разрешено обращаться к серверу DNS.

Другая функция защиты позволяет указать дополнительные серверы, которым будет разрешено копировать информацию с основного сервера DNS. Сервер будет принимать запросы на копирование только от тех дополнительных серверов, которые указаны в списке.

- Убедитесь, что права на изменение конфигурации сервера DNS есть лишь у тех пользователей, которым они действительно необходимы. В противном случае злоумышленник может добавить в файл DNS запись об IP-адресе внешней сети. После этого компьютер с указанным IP-адресом сможет играть роль сервера из защищенной сети, и злоумышленник может получить конфиденциальную информацию от пользователей, подключившихся к этому серверу.

Рекомендации по защите HTTP server for iSeries

Сервер HTTP предоставляет клиентским Web-браузерам доступ к мультимедийным объектам сервера iSeries, в том числе к документам HTML. Он также поддерживает спецификацию *Common Gateway Interface (CGI)*. Прикладные программисты могут расширить набор функций сервера, написав собственные программы CGI.

С помощью Internet Connection Server или IBM HTTP server for iSeries администратор может запустить в системе iSeries сразу несколько серверов. В этом случае каждый активный сервер называется **экземпляром сервера**. Каждому экземпляру сервера присваивается уникальное имя. Администратор может запускать экземпляры и завершать их работу, а также запрещать выполнение некоторых операций отдельным экземплярам.

Примечание: Для настройки и администрирования любого из перечисленных ниже продуктов с помощью Web-браузера нужно запустить экземпляр *ADMIN сервера HTTP:

- Firewall для iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for iSeries

Пользователь (посетитель Web-сайта) не видит меню входа в систему iSeries. Однако администратор сервера iSeries должен явно разрешить применение всех документов HTML и программ CGI, определив их в директивах HTTP. Кроме того, для некоторых или всех запросов администратор может настроить как защиту ресурсов, так и идентификацию пользователей (с помощью ИД пользователя и пароля).

Некоторые атаки злоумышленников приводят к помехам в работе Web-сервера. Сервер может обнаружить атаку такого типа, измеряя тайм-аут запросов некоторых клиентов. Если сервер не получает запрос от клиента, он считает, что выполняется атака с целью помешать работе сервера. Тайм-аут устанавливается после подключения клиента к серверу. По умолчанию сервер обнаруживает атаку и применяет соответствующие меры по ее предотвращению.

Ограничение доступа к системе через HTTP

Для того чтобы *полностью запретить* доступ к системе через HTTP, запретите запуск сервера HTTP. Для этого выполните следующие действия:

__ Шаг 1. Отключите автоматический запуск заданий сервера HTTP при запуске TCP/IP командой:

```
CHGHTTPA AUTOSTART(*NO)
```

Примечания:

a. AUTOSTART(*NO) - это значение по умолчанию.

b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

__ Шаг 2. По умолчанию задание сервера HTTP применяет пользовательский профайл QTMHHTTP. Для того чтобы запретить запуск сервера HTTP, измените состояние пользовательского профайла QTMHHTTP на *DISABLED.

Управление доступом к серверу HTTP

Основная задача сервера HTTP состоит в предоставлении доступа извне к Web-сайту, расположенному в системе iSeries. Посетителя Web-сайта можно сравнить с читателем, просматривающим рекламные объявления в журнале. Такой посетитель не имеет представления об аппаратном и программном обеспечении, благодаря которому работает Web-сайт. В частности, ему ничего не известно ни о типе вашего сервера, ни о его физическом расположении. Обычно пользователям не требуется выполнять никакие дополнительные действия при обращении к Web-сайту (например, им не нужно заполнять меню входа в систему). Однако вы можете ограничить доступ к некоторым документам и программам CGI, предоставляемым Web-сайтом.

Одна система iSeries может предоставлять несколько Web-сайтов. Предположим, что система iSeries поддерживает несколько филиалов вашей компании, каждый из которых обслуживает свою группу заказчиков. Для каждого из этих филиалов можно создать свой Web-сайт, который с точки зрения его посетителей будет полностью независимым от остальных. Кроме того, вы можете создать локальные Web-сайты, содержащие конфиденциальную информацию о работе вашей компании.

Администратор защиты должен защитить Web-сайт, но так, чтобы не слишком ограничить возможности пользователей. Кроме того, он должен убедиться, что работа сервера HTTP не подвергает опасности целостность системы и сети. В приведенных ниже разделах приведены советы по организации защиты системы, в которой установлена эта программа.

Рекомендации по администрированию

Ниже приведены некоторые рекомендации по организации защиты, связанные с администрированием сервера Internet.

- Все действия по настройке выполняются с помощью Web-браузера и экземпляра сервера *ADMIN. Некоторые функции, например, создание дополнительных экземпляров сервера, можно выполнять *только* с помощью сервера *ADMIN.
- Адрес домашней страницы, предназначенной для администрирования (домашней страницы сервера *ADMIN), указан в документации по продуктам, позволяющим выполнять задачи администрирования через интерфейс браузера. Следовательно, любой человек может узнать этот адрес и опубликовать его в конференции, точно так же, как в конференциях публикуются пароли по умолчанию для пользовательских профайлов, поставляемых фирмой IBM. Существует несколько способов защиты от такой атаки:
  - Запускайте экземпляр *ADMIN сервера HTTP только для выполнения административных функций. Не оставляйте его активным все время.
  - Включите поддержку SSL для экземпляра *ADMIN (с помощью Диспетчера цифровых сертификатов). Экземпляр *ADMIN запрашивает ИД пользователя и пароль на основании директив защиты HTTP. Если применяется SSL, ИД пользователя и пароль передаются в зашифрованном виде (как и вся остальная информацию о конфигурации, которая указана в формах администрирования).

– Установите брандмауэр, чтобы запретить доступ к серверу *ADMIN из Internet и скрыть имя системы и имя домена, входящие в состав URL.

- Для выполнения административных функций нужно войти в систему под именем пользователя со специальными правами доступа *IOSYSCFG. Кроме того, вам могут потребоваться права доступа к отдельным объектам системы, в том числе:
  – Библиотекам и каталогам, содержащим документы HTML и программы CGI.
  – Всем пользовательским профайлам, которые вы планируете указать в директивах защиты сервера.
  – Спискам управления доступом (ACL), защищающим каталоги, которые применяются директивами защиты.
  – Контрольному списку - для создания и изменения ИД пользователей и паролей.

  Запустив сервер *ADMIN и протокол TELNET, вы можете выполнять функции администрирования с удаленного компьютера, например, через Internet. Если для администрирования вы применяете общий канал связи (Internet), существует вероятность перехвата ИД пользователя и пароля. Злоумышленник может использовать этот ИД пользователя и пароль для несанкционированного доступа к системе, например, по соединению TELNET или FTP.

  Примечания:

  1. При доступе к системе по соединению TELNET меню Вход в систему рассматривается как обычное меню. Хотя при вводе пароля он не отображается на экране, система передает пароль открытым текстом.
  2. При работе с сервером *ADMIN пароль кодируется, но не шифруется. Кодирование выполняется по стандартной, а следовательно, широко известной схеме. При наличии соответствующих программных инструментов злоумышленник, перехвативший пароль, сможет его раскодировать.

  Совет по организации защиты

  Если вы планируете выполнять задачи администрирования с удаленного компьютера, подключившись через Internet, применяйте экземпляр сервера *ADMIN с поддержкой SSL, чтобы все данные передавались в зашифрованном виде. Не применяйте незащищенные приложения, в частности, TELNET версии ниже V4R4 (TELNET поддерживает SSL начиная с версии V4R4). Если сервер *ADMIN применяется в локальной сети, всем пользователям которой вы *доверяете*, использовать SSL не обязательно.

- Директивы HTTP управляют всей работой сервера. В конфигурации, поставляемой вместе с сервером, разрешен доступ только к начальной странице. До тех пор пока администратор не определит директивы для сервера, клиенты смогут просматривать только начальную страницу. Для определения директив воспользуйтесь интерфейсом Web-браузера для доступа к серверу *ADMIN, либо вызовите команду Работа с конфигурацией HTTP (WRKHTTPCFG). В обоих случаях необходимы специальные права доступа *IOSYSCFG. После подключения сервера iSeries к Internet просмотрите еще раз список пользователей, у которых есть права доступа *IOSYSCFG, и выясните, кому из них они действительно необходимы.

Защита ресурсов

В IBM HTTP server for iSeries предусмотрены директивы HTTP, позволяющие установить надежный контроль за использованием информации сервером. С помощью этих директив можно задать каталоги, в которых Web-сервер может выполнять поиск файлов HTML и программ CGI, переключиться на другой пользовательский профайл iSeries и запросить права доступа к некоторым ресурсам.

Примечание: Подробное описание всех директив HTTP можно найти в разделе ″Web-серверы″ справочной системы Information Center. Ниже приведены некоторые рекомендации по использованию этих директив:

- Сервер HTTP проверяет наличие явных прав доступа. Сервер принимает запрос только в том случае, если последний явно определен в директивах. Другими словами, сервер немедленно отклоняет запрос, если в нем задан URL, отсутствующий в директивах (сервер пытается найти имя или шаблон).
- Директивы защиты позволяют установить режим обязательной идентификации перед предоставлением доступа к ресурсам системы.
  - Когда пользователь (клиент) запрашивает доступ к защищенному ресурсу, сервер отправляет браузеру приглашение на ввод ИД пользователя и пароля. Браузер запрашивает у пользователя ИД пользователя и пароль и отправляет полученную информацию на сервер. Некоторые браузеры сохраняют эту информацию и автоматически отправляют ее в ответ на все последующие запросы. Таким образом, пользователю не приходится вводить один и тот же ИД и пароль в ответ на каждый запрос.

    Если браузер сохраняет ИД пользователя и пароль, возникает та же ситуация, что и в случае с входом пользователей в систему через маршрутизатор или через меню Вход в систему сервера iSeries. Неконтролируемое соединение с браузером предоставляет потенциальную угрозу безопасности системы.
  - Существует три варианта обработки ИД пользователей и паролей, указанных в директивах защиты:
    1. Может выполняться обычная процедура проверки пароля и пользовательского профайла сервера iSeries. Эта процедура чаще всего применяется для защиты ресурсов в корпоративной сети (защищенной сети).
    2. Можно создать ″пользователей Internet″. Такие пользователи идентифицируются сервером iSeries, но у них нет пользовательского профайла. Для управления доступом пользователей Internet создается специальный объект сервера iSeries, который называется ″контрольный список″. Он содержит перечень пользователей, которым разрешено работать с конкретным приложением, и соответствующих паролей.

       Вы можете выбрать способ создания списка ИД пользователей и паролей (например, он может задаваться приложением или пополняться администратором при получении запроса по электронной почте), а также способ его применения. Соответствующую информацию вы можете указать с помощью интерфейса браузера сервера HTTP.

       При работе в незащищенной сети (Internet) создание пользователей Internet обеспечивает более надежную защиту по сравнению с обычными пользовательскими профайлами и паролями. Список уникальных ИД и паролей содержит встроенное ограничение на набор операций, которые могут выполняться пользователями. Пользователи с указанными ИД и паролями не могут войти в систему стандартным способом (например, с помощью TELNET или FTP). Кроме того, в этом случае имена и пароли обычных пользователей не могут быть перехвачены.
    3. Простой протокол доступа к каталогам (LDAP) - это протокол службы каталогов, который предоставляет доступ к каталогу по соединениям TCP. Он позволяет хранить информацию в этой службе каталогов и запрашивать ее. Кроме того, теперь LDAP может применяться и для идентификации пользователей.

    Примечания:

    1. Браузер отправляет имя и пароль пользователя (пользователя Internet или пользователя iSeries) в закодированном, но не в зашифрованном виде. Кодирование выполняется по стандартной, а следовательно, широко

известной схеме. При наличии соответствующих программных инструментов злоумышленник, перехвативший имя и пароль, сможет их раскодировать.

2. Контрольный список хранится в защищенной области памяти системы сервера iSeries. Доступ к нему возможен только через предопределенные системные интерфейсы (API) и только при наличии соответствующих прав доступа.

– С помощью Диспетчера цифровых сертификатов (DCM) вы можете создать собственную сертификатную компанию. Диспетчер цифровых сертификатов автоматически связывает сертификат с пользовательским профайлом его владельца. Следовательно, сертификат предоставляет те же права доступа, что и соответствующий профайл.

- При поступлении запроса на сервер применяется обычная схема защиты ресурсов iSeries. У пользовательского профайла должны быть права доступа к запрошенному ресурсу (например, к папке или исходному физическому файлу, содержащему документ HTML). По умолчанию задания выполняются под управлением пользовательского профайла QTMHHTTP. С помощью специальной директивы можно переключиться на другой пользовательский профайл. В этом случае при обращении к объектам система будет применять права доступа этого пользовательского профайла. Ниже приведены некоторые рекомендации по использованию этой возможности:
  – Переключение на пользовательский профайл полезно применять в случае, когда сервер поддерживает несколько логических Web-сайтов. Директивы позволяют связать с каждым Web-сайтом свой пользовательский профайл. Это дает возможность применять обычную схему защиты ресурсов iSeries для защиты документов этих сайтов.
  – Функцию переключения на другой пользовательский профайл можно применять в сочетании с контрольным списком. Вначале сервер должен идентифицировать запрос на основании уникального ИД пользователя и пароля (которые не совпадают с ИД пользователя и паролем обычного пользователя iSeries). После этого система переключается на другой пользовательский профайл и применяет обычную схему защиты ресурсов. В этом случае пользователь не знает настоящего имени профайла и, следовательно, не может его использовать для выполнения других операций (например, для подключения по FTP).
- Для выполнения некоторых запросов требуется запустить программу на сервере HTTP. Например, программа может обращаться к данным, хранящимся в системе. Перед запуском программы администратор сервера должен преобразовать полученный адрес в имя пользовательской программы, соответствующей стандартам пользовательского интерфейса CGI. Ниже приведены некоторые рекомендации по работе с программами CGI:
  – Для программ CGI можно задать такие же директивы защиты, как и для документов HTML. Следовательно, перед запуском программы вы можете запросить ИД пользователя и пароль.
  – По умолчанию программы CGI выполняются под управлением пользовательского профайла QTMHHTP1. Перед запуском программы можно переключиться на другой пользовательский профайл. Таким образом, для ресурсов, к которым обращаются программы CGI, может применяться обычная схема защиты ресурсов iSeries.
  – Перед предоставлением права на запуск программы CGI в системе администратор защиты должен ознакомиться с этой программой. Он должен знать, откуда получена эта программа и какие функции она выполняет. Кроме того, следует выяснить, какие права доступа есть у пользовательских профайлов, под управлением которых выполняются программы CGI. Все программы CGI необходимо протестировать. Например, необходимо

проверить, можно ли с их помощью получить доступ к командной строке. Все программы CGI следует проверять столь же тщательно, как и программы, принимающие права доступа.

– Убедитесь, что общие права доступа ко всем конфиденциальным объектам ограничены. В некоторых случаях плохо написанная программа CGI может позволить опытному пользователю получить доступ ко всей системе.

– Все программы CGI следует хранить в отдельной пользовательской библиотеке, например, CGILIB. С помощью прав доступа к объектам вы можете указать, кому разрешено добавлять объекты в эту библиотеку и запускать программы из нее. С помощью соответствующих директив вы можете запретить серверу HTTP запускать программы CGI, хранящиеся в других библиотеках.

Примечание: Если сервер предоставляет несколько логических Web-сайтов, вы можете создать библиотеку программ CGI для каждого из них.

Прочие рекомендации по защите

Ниже приведены дополнительные рекомендации по организации защиты:

- Сервер HTTP разрешает лишь чтение объектов iSeries. С помощью запросов к серверу HTTP нельзя напрямую обновить или удалить данные из системы. Однако это можно сделать с помощью программ CGI. Вы можете разрешить программе CGI Net.Data доступ к базе данных сервера iSeries. Для проверки запросов к программе Net.Data система применяет сценарий (аналогичный программе выхода). С его помощью системный администратор может ограничить набор операций, которые будет разрешено выполнять программе Net.Data.
- Сервер HTTP позволяет вести протокол доступа, в который заносится информация об удачных и неудачных попытках обращения к серверу.

Рекомендации по применению SSL для защиты соединений IBM HTTP Server for iSeries

IBM HTTP Server for iSeries предоставляет возможность устанавливать защищенные соединения с Web-сервером iSeries. Web-сайт называется **защищенным** в том случае, если вся информация передается между клиентом и сервером в зашифрованном виде. Шифрование обеспечивает защиту передаваемой информации как от перехвата, так и от копирования и изменения.

Примечание: Обратите внимание, что защита Web-сайта распространяется только на информацию, передаваемую между клиентом и сервером. Она не защищает сам сервер от злоумышленников. Однако такая защита существенно ограничивает объем информации, которую злоумышленники могут получить путем перехвата.

Полная информация об установке и настройке средств шифрования, а также о работе с ними приведена в разделах Information Center, посвященных SSL и Web-серверу (HTTP). В этих разделах приведен обзор функций сервера и перечислены некоторые рекомендации по работе с сервером.

Internet Connection Server поддерживает протоколы HTTP и HTTPS, если установлена одна из следующих лицензионных программ:

- 5722–NC1
- 5722–NCE

В этом случае он называется Internet Connection Secure Server.

Продукт IBM HTTP Server for iSeries (5722–DG1) поддерживает как протокол HTTP, так и протокол HTTPS. Для работы с SSL нужно установить одно из следующих средств шифрования:

- 5722–AC2
- 5722–AC3

Для применения защиты путем шифрования должны быть выполнены следующие требования:

- И отправитель, и получатель (сервер и клиент) должны поддерживать шифрование. Клиент, подключающийся к серверу HTTP, должен поддерживать SSL. (Наиболее популярные Web-браузеры поддерживают SSL). Лицензионные программы шифрования для iSeries поддерживают несколько стандартных способов шифрования. При настройке защищенного сеанса клиент и сервер путем согласования выбирают наиболее надежный из тех способов шифрования, которые они оба поддерживают.
- Данные, передаваемые по соединению, должны быть защищены таким образом, чтобы перехвативший их злоумышленник не смог их расшифровать. Поэтому каждая из сторон шифрует данные своим **личным ключом**, известным только ей. При создании защищенного *внешнего* Web-сайта вы должны получить у независимой сертификатной компании (CA) цифровые сертификаты для всех пользователей и серверов. В данном случае сертификатная компания выступает в роли доверенного лица.

Шифрование обеспечивает конфиденциальность передаваемых данных. Однако при передаче некоторой конфиденциальной информации, например, финансового характера, дополнительно требуется обеспечить целостность этой информации и идентификацию ее отправителя. Иначе говоря, клиент и (при необходимости) сервер должны быть уверены, что отправителю полученной информации можно доверять и что эта информация не была изменена в процессе передачи. Цифровая подпись, полученная у сертификатной компании (CA), предоставляет гарантию целостности информации и подтверждает личность ее отправителя. В протоколе SSL идентификация выполняется путем проверки цифровой подписи сертификата сервера (и, при необходимости, сертификата клиента).

На шифрование и расшифровку данных затрачивается дополнительное время, что снижает скорость передачи данных. В связи с этим, на сервере iSeries предусмотрена возможность запускать программы как в защищенном, так и в незащищенном режиме. Незащищенный сервер HTTP может предоставлять доступ к документам, не требующим защиты, например, к каталогу продуктов. Адрес таких документов будет начинаться с `http://`. Защищенный сервер HTTP может применяться для доступа к конфиденциальной информации, например, к форме, в которой заказчики вводят номер кредитной карты. Такой сервер будет обслуживать запросы на получение документов, адреса которых начинаются с `http://` или `https://`.

Напоминание

В Internet считается правилом хорошего тона сообщать клиентам о том, будут ли данные передаваться в защищенном режиме, особенно в том случае, если для доступа к некоторым документам через ваш Web-сайт нужно установить защищенное соединение.

Помните, что шифрование может применяться только в том случае, если защищены обе стороны - и клиент, и сервер. В настоящее время большинство браузеров (клиентов HTTP) предоставляют функции защиты.

Рекомендации по настройке защиты LDAP

К функциям защиты протокола LDAP относятся Secure Sockets Layer (SSL), Списки управления доступом и шифрование паролей по алгоритму CRAM-MD5. В выпуске V5R1 для повышения надежности защиты LDAP была добавлена поддержка соединений Kerberos и функция контроля за действиями.

Дополнительная информация по этому вопросу приведена в iSeries Information Center—>Сеть–>TCP/IP–>Службы каталогов (LDAP). Информация о работе с iSeries Information Center приведена в разделе “Необходимая и полезная информация” на стр. xii.

Рекомендации по защите LPD

LPD (демон построчной печати) позволяет передавать вывод на принтер в вашу систему. При работе с LPD вход в систему не выполняется.

Ограничение доступа к LPD

Для того чтобы *полностью запретить* доступ к LPD, запретите запуск сервера LPD. Для этого выполните следующие действия:

__ Шаг 1. Отключите автоматический запуск заданий сервера LPD при запуске TCP/IP командой:

```
CHGLPDA AUTOSTART(*NO)
```

Примечания:

a. AUTOSTART(*YES) - это значение по умолчанию.

b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

__ Шаг 2. Для того чтобы запретить подключение пользовательских приложений, в частности, приложений с API сокетов, к порту, обычно занятому LPD, выполните следующие действия:

__ Шаг a. Введите `GO CFGTCP`. Будет показано меню Настроить TCP/IP.

__ Шаг b. Выберите опцию 4 (Работа с ограничениями на порты TCP/IP).

__ Шаг c. В меню Работа с ограничениями на порты TCP/IP выберите опцию 1 (Добавить).

__ Шаг d. В качестве нижней границы диапазона портов укажите `515`.

__ Шаг e. В качестве верхней границы диапазона портов укажите `*ONLY`.

Примечания:

1) Ограничение на использование порта вступит в силу при следующем запуске TCP/IP. Если во время настройки ограничений на использование порта протокол TCP/IP активен, перезапустите его.

2) Информация о назначении общих номеров портов приведена в RFC1700.

__ Шаг f. В качестве протокола укажите `*TCP`.

__ Шаг g. В поле Пользовательский профайл укажите имя защищенного профайла, определенного в системе. (Защищенным называется пользовательский профайл, которому не принадлежат никакие программы, принимающие права доступа, и пароль которого не известен другим пользователям.) Выделяя порт

конкретному пользователю, вы автоматически запрещаете его применение всем остальным пользователям.

__ Шаг h. Повторите шаги с 2c по 2g для протокола *UDP.

Управление доступом к LPD

Если доступ к системе через LPD необходим, настройте его с учетом следующих рекомендаций по защите:

- Для того чтобы предотвратить переполнение системы ненужными объектами, установите разумные ограничения на пулы вспомогательной памяти (ASP). Просмотреть и изменить эти ограничения можно с помощью Системного инструментария (SST) или Специальных сервисных средств (DST). Дополнительная информация об ограничениях на ASP приведена в книге *Backup and Recovery*.
- Для ограничения возможностей пользователей, которые могут отправлять в систему буферные файлы, настройте права доступа к очередям вывода. Пользователи LPD, у которых нет собственного пользовательского профайла, работают под управлением профайла QTMPLPD. Вы можете ограничить набор очередей вывода, доступных этому профайлу.

Рекомендации по защите системы, применяющей протокол SNMP

Сервер iSeries может играть в сети роль агента Простого протокола управления сетью (SNMP). SNMP предназначен для централизованного управления шлюзами, маршрутизаторами и хостами в сети. Агент SNMP собирает информацию о системе и выполняет запросы удаленного диспетчера сети SNMP.

Ограничение доступа через SNMP

Для того чтобы *полностью запретить* доступ к системе через SNMP, запретите запуск сервера SNMP. Для этого выполните следующие действия:

__ Шаг 1. Отключите автоматический запуск заданий сервера SNMP при запуске TCP/IP командой:

```
CHGSNMPA AUTOSTART(*NO)
```

Примечания:

a. AUTOSTART(*YES) - это значение по умолчанию.

b. Информация об управлении автоматическим запуском серверов TCP/IP приведена в разделе “Управление автоматическим запуском серверов TCP/IP” на стр. 128.

__ Шаг 2. Для того чтобы запретить подключение пользовательских приложений, в частности, приложений с API сокетов, к порту, обычно занятому SNMP, выполните следующие действия:

__ Шаг a. Введите `GO CFGTCP`. Будет показано меню Настроить TCP/IP.

__ Шаг b. Выберите опцию 4 (Работа с ограничениями на порты TCP/IP).

__ Шаг c. В меню Работа с ограничениями на порты TCP/IP выберите опцию 1 (Добавить).

__ Шаг d. В качестве нижней границы диапазона портов укажите `161`.

__ Шаг e. В качестве верхней границы диапазона портов укажите `*ONLY`.

Примечания:

1) Ограничение на использование порта вступит в силу при следующем запуске TCP/IP. Если во время настройки ограничений на использование порта протокол TCP/IP активен, перезапустите его.

2) Информация о назначении общих номеров портов приведена в RFC1700.

__ Шаг f. В качестве протокола укажите *TCP.

__ Шаг g. В поле Пользовательский профайл укажите имя защищенного профайла, определенного в системе. (Защищенным называется пользовательский профайл, которому не принадлежат никакие программы, принимающие права доступа, и пароль которого не известен другим пользователям.) Выделяя порт конкретному пользователю, вы автоматически запрещаете его применение всем остальным пользователям.

__ Шаг h. Повторите шаги с 2c по 2g для протокола *UDP.

Управление доступом через SNMP

Если доступ к системе через SNMP необходим, настройте его с учетом следующих рекомендаций по защите:

- Доступ к сети через SNMP дает возможность собирать информацию о вашей сети. В частности, таким образом может быть получена информация, защищаемая с помощью псевдонимов и сервера имен доменов. Кроме того, SNMP позволяет изменять настройку сети, поэтому несанкционированный доступ к этому протоколу может привести к нарушению ее работы.
- Для доступа к SNMP необходимо знать имя группы взаимодействия. Это имя выполняет те же функции, что и пароль. Имя группы взаимодействия не шифруется. Это означает, что при передаче по линиям связи оно может быть перехвачено. Параметр IP-адрес диспетчера (INTNETADR) команды Добавить взаимодействие для SNMP (ADDCOMSNMP) позволяет указать допустимые IP-адреса диспетчера (значение по умолчанию - *ANY). Кроме того, вы можете указать значение *NONE в параметре OBJACC команды ADDCOMSNMP или CHGCOMSNMP, чтобы запретить диспетчерам группы взаимодействия доступ к объектам MIB. Это позволяет временно запретить доступ к диспетчерам группы взаимодействия без удаления группы.

Рекомендации по настройке защиты сервера INETD

Большинство серверов TCP/IP предоставляют клиентам только одну службу. В отличие от них, сервер INETD предоставляет множество различных служб, которые могут быть настроены администратором. По этой причине сервер INETD иногда называют суперсервером. Сервер INETD предоставляет следующие встроенные службы:

- time
- daytime
- echo
- discard
- changed

Эти службы применимы как к пакетам TCP, так и к пакетам UDP. В случае UDP службы echo, time, daytime и changed получают пакеты UDP и затем отправляют ответные пакеты отправителю. Сервер echo отправляет обратно полученные пакеты без изменения, серверы time и daytime - время в определенном формате, а сервер changed - пакет, содержащий печатаемые символы ASCII.

Эти службы UDP делают систему уязвимой для атак типа ″помехи в работе″. Предположим, что у вас есть два сервера iSeries: SYSTEMA и SYSTEMB. Злоумышленник может сфабриковать заголовок пакета IP или UDP, содержащий

адрес системы SYSTEMA в качестве адреса отправителя и номер порта UDP сервера time. Затем он может отправить этот пакет серверу time системы SYSTEMB, которая отправит время системе SYSTEMA, которая вновь отправит пакет системе SYSTEMB, и так далее до бесконечности. На такой обмен пакетами будет затрачиваться значительная часть процессорного времени в обеих системах и ресурсов сети.

Учитывая возможность подобных атак, такие службы следует запускать только в защищенной сети. В конфигурации, которая поставляется с сервером INETD, опция автоматического запуска вместе с TCP/IP выключена. Вы можете указать, нужно ли запускать службы вместе с сервером INETD. По умолчанию вместе с сервером INETD запускаются серверы time и daytime для протоколов TCP и UDP.

Существует два файла конфигурации сервера INETD:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

В этих файлах указываются программы, которые нужно запускать вместе с сервером INETD, а также пользовательские профайлы, под управлением которых должны выполняться эти программы.

Примечание: Файл конфигурации из каталога proddata изменять не следует. Он обновляется при каждой перезагрузке системы. Все пользовательские изменения можно вносить только в файл из каталога userdata, так как он **не** обновляется при установке нового выпуска.

Если злоумышленник получит доступ к этим файлам, он может добавить в них запись о любой программе, и тогда эта программа будет запускаться вместе с INETD. Следовательно, исключительно важно защитить эти файлы. По умолчанию для изменения этих файлов требуются права доступа QSECOFR. Не следует понижать уровень прав доступа, необходимый для доступа к этим файлам.

Примечание: Не изменяйте файл конфигурации, расположенный в каталоге ProdData. Он обновляется при каждой перезагрузке системы. Все пользовательские изменения могут вноситься только в файл из каталога UserData, так как он не обновляется при установке нового выпуска.

Ограничение перемещения пользователей между системами с помощью TCP/IP

Если ваша система подключена к сети, то вам рекомендуется ограничить перемещение пользователей между системами с помощью приложений TCP/IP. Для этого ограничьте доступ к следующим командам запуска клиентских программ TCP/IP:

Примечание: Эти команды могут находиться в нескольких библиотеках системы. В частности, они есть в библиотеках QSYS и QTCP. Обязательно найдите все копии.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF

- RUNRMTCMD (клиент REXEC)

Целевая система может определяться одним из следующих способов:

- По записи в таблице хостов TCP/IP.
- По записи *DFTROUTE в таблице хостов TCP/IP. Это позволяет определять следующий узел маршрутизации, даже если целевая сеть неизвестна. Маршрут по умолчанию применяется при подключении к удаленным сетям.
- По записи удаленного сервера имен в конфигурации. Это позволяет применять для преобразования имен хостов альтернативный сервер.
- По таблице удаленных систем.

Необходимо ограничить права доступа на изменение перечисленных таблиц и конфигурации. Администратор защиты должен иметь четкое представление о назначении и действии этих параметров.

Учтите, что опытный пользователь, обладающий доступом к компилятору ILE C, может создать программу сокетов, подключающуюся к порту TCP или UDP. Вы можете усложнить ему задачу, запретив доступ к следующим файлам интерфейса сокетов в библиотеке QSYSINC:

- SYS
- NETINET
- H
- ARPA
- Sockets и SSL

Ограничьте доступ к следующим откомпилированным служебным программам работы с сокетами и SSL:

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

Эти службы поставляются с общими правами доступа *USE, но вы можете изменить их на *EXCLUDE (или любое другое значение).

Глава 14. Ограничение доступа пользователей рабочих станций

Многие пользователи системы используют свои персональные компьютеры (PC) в качестве рабочих станций. Они не только работают с программными инструментами, установленными на PC, но и подключаются к серверу iSeries.

Большинство способов подключения PC к серверу iSeries предоставляют более широкий набор функций по сравнению с эмуляцией рабочей станции. PC может предоставлять пользователю меню входа в систему iSeries для установления интерактивного сеанса. Кроме того, PC может играть роль отдельного компьютера и предоставлять такие функции, как передача файлов и вызов удаленных процедур.

Администратор защиты сервера iSeries должен выбрать:

- Функции, которые разрешено запускать пользователям PC, подключившимся к системе
- Ресурсы сервера iSeries, доступ к которым будет предоставляться пользователям PC.

Вы можете запретить использование дополнительных функций PC (таких как передача файлов и вызов удаленных процедур), если на них еще не распространяется схема защиты сервера iSeries. В некоторых случаях конечной целью является разрешить использование дополнительных функций PC и одновременно защитить информацию, хранящуюся в системе. В приведенном ниже разделе обсуждаются некоторые вопросы защиты, связанные с доступом пользователей PC к системе AS/400.

Защита от проникновения вирусов с рабочих станций

В этом разделе описаны способы защиты системы от проникновения вирусов с PC.

Ограничение доступа пользователей рабочих станций к данным

Некоторые клиенты PC хранят данные в общих папках на сервере. Пользователи PC могут обращаться к файлам базы данных iSeries с помощью набора интерфейсов, определенных стандартным образом. С помощью функции передачи файлов, которая предусмотрена в большинстве программ клиент/сервер, пользователи PC могут копировать файлы с сервера и на сервер. С помощью функции доступа к базам данных, например, файлов DDM, удаленного SQL или драйвера ODBC, пользователь PC может работать с данными, хранящимися на сервере.

Если в системе настроены описанные функции, вы можете создать программы, которые будут перехватывать и проверять запросы пользователей PC к ресурсам сервера. Программу выхода для проверки запросов на работу с файлом DDM можно задать в сетевом атрибуте обработки запросов к управлению распределенными данными (DDMACC). Для некоторых способов передачи файлов PC вы можете задать программу выхода в сетевом атрибуте Обработка запросов клиентов (PCSACC). В этом же атрибуте можно задать значение PCSACC (*REGFAC), чтобы применялась функция регистрации. Для обработки запросов на доступ к данным, применяющим другие функции сервера, вы можете зарегистрировать программы выхода с помощью команды WRKREGINF.

Недостатком программ выхода является то, что их тяжело создать самостоятельно, и они редко обеспечивают полную защиту. Программы выхода обеспечивают более слабую защиту, чем права доступа к объектам, которые защищают объекты от несанкционированного доступа любых пользователей.

Для хранения и доступа к данным сервера iSeries некоторые клиентские программы, например, IBM iSeries Access для Windows, применяют интегрированную файловую систему. Интегрированная файловая система упрощает доступ пользователей PC ко всем данным сервера. Следовательно, в этом случае права доступа к объектам играют еще более важную роль. Если у пользователя есть необходимые права доступа, он может просмотреть содержимое библиотеки сервера точно так же, как и содержимое любого каталога PC. С помощью простых команд перемещения и копирования можно мгновенно переносить данные с сервера iSeries на PC и наоборот. Система автоматически преобразует формат данных.

Примечания:

1. Для управления доступом к объектам из файловой системы QSYS.LIB можно создать список прав доступа. Дополнительная информация приведена в разделе “Ограничение доступа к файловой системе QSYS.LIB” на стр. 105.
2. Дополнительные советы по организации защиты, касающиеся интегрированной файловой системы, приведены в разделе Глава 11, “Защита файлов с помощью Интегрированной файловой системы”, на стр. 99.

Основным преимуществом интегрированной файловой системы как для пользователей, так и для разработчиков, является ее простота. С помощью одного интерфейса пользователь может работать с объектами в разных средах. Для доступа к объектам пользователю PC не нужно устанавливать специальное программное обеспечение или API. Он может работать с объектами с помощью хорошо знакомых команд PC или “мыши”.

Для любой системы, к которой подключены PC, и в особенности для системы с клиентскими программами, применяющими интегрированную файловую систему, необходимо разработать продуманную схему защиты объектов. Поскольку функции защиты встроены в операционную систему OS/400, все запросы на доступ к данным проходят через процедуру проверки прав доступа. Проверка прав доступа должна выполняться для всех запросов, независимо от их отправителя и способа доступа к данным.

Права доступа к объектам, предоставляемые пользователям рабочей станции

Устанавливая права доступа к объекту, необходимо проверять, какие права доступа предоставляются пользователям PC. Например, если у пользователя есть права *USE для доступа к файлу, он может просмотреть и напечатать содержимое этого файла. Однако он не может удалить файл или изменить его содержимое. Для пользователя PC просмотр равносилен “чтению” файла. Это означает, что пользователь сможет скопировать файл на PC, что не всегда желательно.

Для того чтобы запретить загрузку файлов, содержащих конфиденциальную информацию, установите для них общие права доступа *EXCLUDE. После этого предоставьте другую возможность для “просмотра” файла на сервере, например, с помощью меню и программ, принимающих права доступа.

Другой способ запретить загрузку файла заключается в создании программы выхода, которая запускается, когда пользователь PC вызывает любую функцию сервера (отличную от меню входа в систему). Такую программу выхода можно задать в

сетевом атрибуте PCSACC с помощью команды Изменить сетевой атрибут (CHGNETA). Кроме того, вы можете зарегистрировать программы выхода с помощью команды Работа с информацией о регистрации (WRKREGINF). Выберите один из способов задания программы выхода в зависимости от способа доступа к данным, применяемого пользователями PC, и типа клиентских программ, установленных на PC. Программа выхода (QIBM_QPWFS_FILE_SERV) при обращении к IFS с помощью iSeries Access и NetServer. Она не запрещает доступ пользователей PC другими способами, например, по FTP или через ODBC.

Обычно помимо функции загрузки данных из системы программы PC предоставляют функцию передачи данных в систему, с помощью которой пользователь может скопировать данные из PC в файл базы данных сервера. Если вы не предусмотрите такую возможность в своей схеме защиты, пользователь PC может полностью заменить содержимое файла. Предоставляйте права доступа *CHANGE лишь тогда, когда они действительно необходимы. Права доступа, необходимые для выполнения различных операций над файлами, перечислены в приложении D книги *iSeries Security Reference*.

Дополнительная информация о правах доступа, которые следует предоставлять функциям PC, а также о программах выхода приведена в iSeries Information Center. Подробные сведения приведены в разделе “Необходимая и полезная информация” на стр. xii.

Администрирование приложений

Администрирование приложений - это необязательный компонент Навигатора iSeries, графического пользовательского интерфейса (GUI) для сервера iSeries. Этот компонент позволяет системным администраторам управлять функциями или приложениями, доступными для пользователей конкретного сервера. В том числе, с его помощью можно ограничить набор функций, доступных пользователям, применяющим для работы с сервером клиентские программы. Необходимо отметить, что при подключении к серверу через клиент Windows набор доступных функций администрирования определяется правами доступа пользователя iSeries, а не правами доступа пользователя Windows.

Дополнительная информация о компоненте Администрирование приложений программы Навигатор iSeries приведена в разделе iSeries Information Center –> Подключение к iSeries—>Способы подключения —> Навигатор iSeries (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Управление стратегиями

Стратегии разрабатываются и используются администраторами при настройке программного обеспечения на компьютерах-клиентах. С их помощью можно ограничить набор функций и приложений, доступных пользователям этих PC. Стратегии также могут задавать рекомендуемые или обязательные конфигурации для работы конкретных пользователей на конкретных PC.

Примечание: Стратегии не позволяют управлять ресурсами сервера. Они не являются инструментами защиты сервера. С помощью стратегий можно определить параметры доступа к серверу через iSeries Access для конкретного пользователя и конкретного компьютера. Стратегии не ограничивают доступ к ресурсам сервера с помощью других инструментов.

Стратегии хранятся на файловом сервере. При каждом входе пользователя в систему с рабочей станции Windows соответствующие стратегии загружаются с файлового сервера. Эти стратегии загружаются в реестр до того, как пользователь начнет работу с персональным компьютером.

Стратегии Microsoft и Администрирование приложений

iSeries Access Express поддерживает два способа администрирования систем в сети: системные стратегии Microsoft и средства администрирования приложений программы Навигатор iSeries. Приведенная ниже информация поможет вам выбрать наиболее подходящий способ.

Системные стратегии Microsoft

Эти стратегии разработаны для PC и не зависят от установленных выпусков OS/400. Стратегии могут быть заданы как для PC, так и для пользователей Windows. Это означает, что будут применяться профили пользователей Windows, а не профайлы пользователей сервера. Стратегии можно применять для задания конфигурации и ограничений. В целом, стратегии позволяют выполнить более точную настройку более широкого набора функций, чем Администрирование приложений. Это связано с тем, что для проверки прав доступа пользователя к функции устанавливать соединение с сервером не нужно. Работать со стратегиями сложнее, чем с Администрированием приложений, поскольку для стратегий требуется специальный редактор Microsoft, а поддержку стратегий необходимо настраивать отдельно на каждом PC.

Функция Администрирование приложений программы Навигатор iSeries

В отличие от системных стратегий Microsoft, Администрирование приложений применяет пользовательские профайлы, а не профили Windows. Хотя Администрирование приложений может применяться для работы со всеми серверами iSeries, на которых установлен продукт OS/400 версии V4R3 и старше, некоторые функции доступны только в версиях не ниже V4R4. Для работы с Администрированием приложений применяется графический пользовательский интерфейс программы Навигатор iSeries, который намного удобнее, чем редактор стратегий. Информация Администрирования приложений применяется для пользователя независимо от того, с какого PC он вошел в систему. Может быть запрещен доступ к некоторым функциям Навигатора iSeries. Администрирование приложений рекомендуется применять в том случае, когда все функции, для которых вам нужно задать ограничения, поддерживаются Администрированием приложений, а в системе установлена OS/400 версии V4R3 или выше.

Применение SSL в iSeries Access для Windows

Информация о применении SSL в программе iSeries Access Express приведена в следующих разделах iSeries Information Center: *Администрирование SSL, Защита iSeries Access Express и Навигатора iSeries Navigator, iSeries Developer Kit for Java, а также iSeries Java Toolbox* в разделе Java. Эта информация также поставляется вместе с системой на компакт-диске.

Функции защиты Навигатора iSeries

Навигатор iSeries предоставляет простой интерфейс для работы с сервером тем пользователям, которые применяют iSeries Access. С каждым выпуском OS/400 все больше функций сервера становится доступно в Навигаторе iSeries. У простого интерфейса есть много преимуществ, в том числе низкая стоимость технической

поддержки и большая привлекательность для пользователей. Одновременно с этим, он предъявляет дополнительные требования к защите.

Администратор защиты должен защитить ресурсы от пользователей. Навигатор iSeries предоставляет пользователям доступ ко многим функциям и значительно упрощает работу с ними. Проверьте, что разработанные и реализованные стратегии защиты пользовательских профайлов и объектов соответствуют предъявляемым требованиям.

В продукте IBM e(logo)Server iSeries Access для Windows выпуска V4R4 и старше предусмотрены следующие способы ограничения доступа пользователей к функциям Навигатора iSeries:

- Выборочная установка
- Администрирование приложений
- Поддержка системных стратегий Windows NT

Навигатор iSeries поставляется в виде набора компонентов, которые можно устанавливать независимо друг от друга. Это позволяет заказчикам устанавливать только те компоненты, которые им необходимы. Компонент Администрирование приложений позволяет администратору ограничить доступ пользователей и групп к функциям Навигатора iSeries. В Администрировании приложений все приложения разбиты на следующие группы:

Навигатор iSeries
К этой группе относятся Навигатор iSeries и все встраиваемые модули

Клиентские приложения
К этой группе относятся все остальные клиентские приложения (в том числе iSeries Access), предоставляющие функции, которыми можно управлять с помощью Администрирования приложений.

Приложения хоста
К этой группе относятся все приложения, расположенные на сервере и предоставляющие функции, для управления которыми применяется Администрирование приложений.

С помощью выборочной установки, функции Администрирование приложений и стратегий можно ограничить доступ пользователей к функциям Навигатора iSeries. Однако ни одна из этих функций не подходит для защиты ресурсов.

Начиная с выпуска V4R4, продукт IBM e(logo)server iSeries Access для Windows поддерживает редактор системных стратегий Windows NT, позволяющий ограничить набор функций, которые разрешено выполнять всем пользователям указанного PC.

Дополнительная информация о выборочной установке, функции Администрирование приложений и функции Управление стратегиями приведена в справочной документации iSeries Information Center. Некоторые сведения об администрировании приложений приведены и в разделе “Ограничение доступа к функции программы” на стр. 5 данной книги.

Ограничение доступа к ODBC

ODBC - это средство, позволяющее приложениям PC работать с данными системы iSeries как с локальными. Программист ODBC может сделать физическое расположение данных несущественным для приложения персонального компьютера. Рекомендации по защите ODBC приведены в документе ″iSeries Access for Windows ODBC security″ (/rzaii/rzaiiodbc09.HTM), входящем в состав iSeries Information Center.

Рекомендации по применению паролей в сеансах рабочей станции

Обычно при запуске программы, устанавливающей соединение, например, iSeries Access, пользователь вводит ИД и пароль, запрашиваемые сервером. После этого пароль зашифровывается и сохраняется в памяти PC. Когда пользователь вновь подключается к тому же серверу, PC автоматически отправляет ИД пользователя и пароль.

В некоторых программах клиент/сервер предусмотрена опция пропуска меню Вход в систему при установлении интерактивных сеансов. Если эта опция будет выбрана, перед открытием интерактивного сеанса (эмуляции 5250) программа автоматически отправит ИД пользователя и зашифрованный пароль. Для применения этой функции установите системное значение QRMTSIGN на сервере равным *VERIFY.

Перед выбором опции пропуска меню Вход в систему следует оценить влияние этой опции на защиту системы.

Возможная опасность: В сеансе эмуляции 5250 и любом другом интерактивном сеансе меню Вход в систему ничем не отличается от остальных меню. Хотя пароль и не отображается при вводе, он передается по соединению в незашифрованном виде, как и любое другое поле данных. Для некоторых типов соединений существует возможность копирования данных, передаваемых по соединению, в том числе ИД пользователя и пароля. Копирование данных, передаваемых по соединению, с помощью электронного оборудования часто называют **перехватом**. В выпуске V4R4 и более поздних для защиты соединений, устанавливаемых между iSeries Access и сервером iSeries, может применяться протокол SSL. Такие соединения защищают данные, в том числе и пароли, от перехвата.

Если опция пропуска меню Вход в систему выбрана, пароль зашифровывается на PC до передачи по соединению. Шифрование исключает возможность получения готового пароля путем перехвата. Помимо защиты пароля необходимо убедиться, что пользователи PC применяют функции защиты во время работы. Сеанс с системой iSeries, открытый на автономном PC, дает возможность любому пользователю открыть другой сеанс без ввода ИД пользователя и пароля. Если компьютер простаивает в течение длительного периода времени, сеанс с системой должен блокироваться. При возобновлении сеанса должен запрашиваться пароль.

Даже если опция пропуска меню Вход в систему не выбрана, активный сеанс на автономном PC представляет потенциальную угрозу безопасности системы. С помощью программ PC пользователь может запустить сеанс работы с сервером и получить доступ к данным системы, не вводя ИД пользователя и пароль. Поскольку в сеансе эмуляции 5250 легче всего открыть новый сеанс для работы с данными системы, то вероятность несанкционированного доступа в таком сеансе выше, чем в любом другом сеансе.

Проинформируйте пользователей о том, что происходит при отключении сеанса iSeries Access. Логично предположить, что при выборе опции отключения соединение с сервером прерывается, однако это не так. На самом деле при выборе опции отключения сервер предоставляет сеанс пользователя (лицензию) другим пользователям. При этом соединение с сервером не прерывается. Следовательно, пользователь, работающий на незащищенном PC, может получить доступ к ресурсам сервера, не вводя ИД пользователя и пароль.

Можно предложить два варианта отключения сеанса:

- Убедитесь, что на PC настроена функция блокировки сеанса, запрашивающая пароль при возобновлении сеанса. Это позволит защитить автономный PC от несанкционированного доступа.
- Для того чтобы полностью завершить сеанс, завершите работу Windows или перезагрузите PC. В этом случае сеанс связи с системой iSeries будет завершен.

Кроме того, проинформируйте пользователей о том риске, с которым связано применение программы iSeries Access для Windows. Когда пользователь указывает имя ресурса iSeries в формате UNC (универсальное соглашение о присвоении имен), клиент Win95 или NT подключается к серверу. Имя в формате UNC позволяет скрыть, что на самом деле пользователь обращается к подключенному сетевому диску. Чаще всего пользователь даже не подозревает о том, что было установлено сетевое соединение. Тем не менее, если соединение было установлено на незащищенном PC, оно предоставляет угрозу безопасности сервера, так как все данные сервера будут показаны на PC в виде дерева каталогов. Если сеанс был установлен от имени пользовательского профайла, которому предоставлены многие права доступа, то пользователь незащищенного PC сможет получить доступ к ресурсам сервера. Как и в предыдущем примере, для предотвращения такой ситуации нужно проинформировать пользователей о вероятности несанкционированного доступа и убедиться, что на PC настроена функция блокировки.

Запрет на запуск удаленных команд и процедур на сервере

С помощью таких программ как iSeries Access опытные пользователи PC могут запускать команды на сервере, минуя меню Вход в систему. Ниже перечислено несколько способов запуска команд на сервере, которые есть у пользователей PC. Какой из этих способов может применяться в вашем случае, зависит от программы клиент/сервер, установленной на PC.

- Для запуска команды пользователь может открыть файл DDM и вызвать функцию удаленной команды.
- Некоторые программы, в том числе оптимизированные клиенты iSeries Access, позволяют запускать удаленные команды с помощью API Вызов распределенных программ (DPC), который не использует DDM.
- Некоторые программы, например, удаленный SQL и ODBC, позволяют запускать удаленные команды с помощью DDM или DPC.

Если для запуска удаленных команд в программе клиент/сервер применяется DDM, вы можете запретить запуск всех удаленных команд с помощью сетевого атрибута DDMACC. Если в программе клиент/сервер применяется другая функция сервера, вы можете зарегистрировать программу выхода для этого сервера. Если вы планируете разрешить запуск удаленных команд, проверьте, что установленные права доступа обеспечивают достаточную защиту объектов. Разрешение запуска удаленных команд равносильно предоставлению пользователю командной строки. Обратите внимание, что при получении запроса на запуск удаленной команды через DDM система iSeries не устанавливает в пользовательском профайле опцию ограничения возможностей (LMTCPB).

Запрет на запуск удаленных команд и процедур на рабочей станции

Программа IBM iSeries Access для Windows позволяет запускать удаленные команды на PC. Для запуска процедуры на подключенном PC на сервере нужно вызвать команду Запустить удаленную команду (RUNRMTCMD). Команда RUNRMTCMD чрезвычайно полезна для системных администраторов и работников службы поддержки. Однако с ее помощью могут быть повреждены данные PC, намеренно или случайно.

На PC нет функций проверки прав доступа к объектам, аналогичных функциям сервера iSeries. Для того чтобы избежать негативных последствий запуска команды RUNRMTCMD, ограничьте доступ к этой команде на сервере. Программа IBM iSeries Access для Windows позволяет зарегистрировать пользователей, которым разрешено запускать удаленные команды на заданном PC. Для управления доступом к функции запуска удаленных команд по соединению TCP/IP можно воспользоваться свойствами панели управления. Вы можете предоставить права на запуск команд пользователю с определенным ИД или пользователям конкретной удаленной системы. В случае соединения SNA некоторые клиентские программы позволяют настроить защиту диалога. В остальных программах можно лишь разрешить или запретить получение удаленных команд.

Учитывая то, какая клиентская программа установлена на PC и какой тип соединения применяется (TCP/IP или SNA), оцените риск, связанный с запуском удаленных команд на подключенных PC. Ознакомьтесь с дополнительной информацией, приведенной в документации по клиентской программе, путем поиска слов “удаленная команда” и “RUNRMTCMD”. Подготовьте для пользователей PC и сетевых администраторов советы по организации защиты клиентов в случае, когда запуск удаленных команд должен быть разрешен или запрещен.

Шлюзы

Персональные компьютеры могут подключаться к системе iSeries через промежуточный сервер, или шлюз. Например, система iSeries может быть подключена к локальной сети, содержащей сервер PC, к которому подключены PC. В такой ситуации схема защиты зависит от программного обеспечения, запущенного на сервере шлюза. Пример конфигурации со шлюзом приведен на рис. 13:

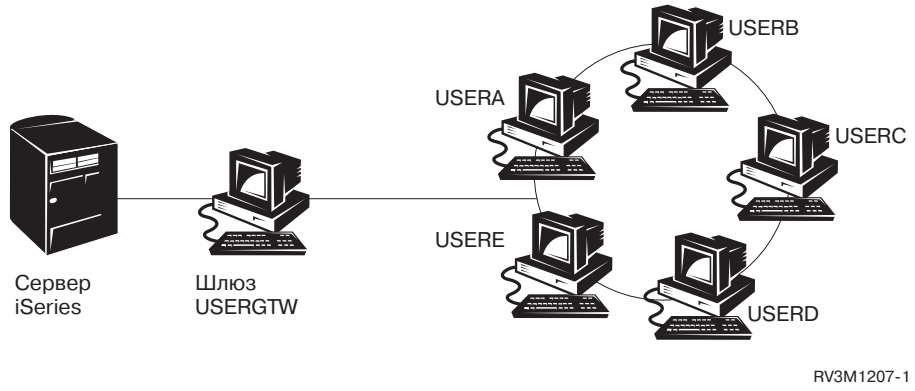

Рисунок 13. Система iSeries со шлюзом

В случае некоторых программ система iSeries ничего не знает о пользователях (например, USERA или USERC), расположенных за сервером шлюза. Сервер входит в систему как некоторый пользователь (USERGTW). Для обработки всех запросов пользователей, расположенных за шлюзом, будет применяться ИД пользователя USERGTW. Запрос пользователя USERA будет рассматриваться системой как запрос пользователя USERGTW.

В данном случае все действия по защите должны выполняться сервером шлюза. Вы должны ознакомиться с функциями защиты сервера шлюза и настроить их. На сервере iSeries всем пользователям будут предоставляться те же права доступа, что и пользователю с ИД, указанным сервером шлюза при запуске сеанса. Это эквивалентно запуску программы, перенимающей права доступа и предоставляющей командную строку.

В других программах сервер шлюза передает запросы отдельных пользователей на сервер iSeries. В этом случае сервер iSeries знает, что к объекту обращается пользователь USERA. Шлюз не изменяет запросы к системе.

Если система подключена к сети, в которой есть сервер шлюзов, оцените, какие права доступа нужно предоставить ИД сервера шлюза. Кроме того, вам нужно получить следующую информацию:
- Какие способы защиты предусмотрены на сервере шлюза.
- Какой способ представления пользователей, расположенных за шлюзом, будет применяться в системе iSeries.

Беспроводные локальные сети

iSeries Wireless LAN обеспечивает беспроводное подключение клиентов к системе iSeries. Для установления беспроводного соединения используются радиоволны. Администратору защиты должны быть известны следующие особенности продуктов iSeries Wireless LAN:

- Для создания беспроводной локальной сети применяется технология широкополосной связи. Ранее эта технология применялась правительством США для защищенного радиообмена. Для внешнего наблюдателя широкополосная передача больше похожа на естественный шум, чем на передачу данных.
- Защиту беспроводного соединения обеспечивают три параметра конфигурации:
  - Скорость передачи данных (две возможные скорости)
  - Частота (пять возможных частот)
  - Идентификатор системы (8 миллионов возможных идентификаторов)

  Значения этих параметров образуют 80 миллионов возможных конфигураций, так что вероятность угадывания правильной конфигурации с целью подслушивания пренебрежимо мала.
- Как и в других технологиях передачи информации, защита беспроводных соединений во многом зависит от защиты клиентского устройства. Идентификатор системы и прочие параметры конфигурации хранятся в файле клиентского устройства, который должен быть защищен.
- В случае утери или кражи беспроводного устройства обычные средства защиты сервера, такие как пароли входа в систему и защита объектов, предотвратят несанкционированное использование этого устройства для получения доступа к системе.
- Несмотря на это, в этом случае рекомендуется изменить идентификаторы всех пользователей, точек доступа и систем. Это действие аналогично смене всех замков в случае потери ключей.
- Рекомендуется также разделять клиентов на группы с различными идентификаторами. Это позволяет сократить объем операций по защите, выполняемых при утере или краже одного устройства. Данный способ пригоден только в том случае, когда существуют группы пользователей, работающих в некоторой подобласти пространства связи.
- В отличие от проводных локальных сетей, беспроводная технология запатентована. Это означает, что перехватчики сигнала беспроводных локальных сетей отсутствуют в свободной продаже. Перехватчиком сигнала называется электронное устройство, позволяющее несанкционированно принимать передаваемую информацию.

Глава 15. Программы выхода для защиты

В некоторых функциях сервера iSeries предусмотрены точки выхода для запуска пользовательских программ, выполняющих дополнительную проверку. Например, вы можете настроить систему таким образом, чтобы она запускала программу выхода при попытке пользователя открыть файл DDM (управление распределенными данными). Для того чтобы задать программы выхода, которые должны запускаться при выполнении определенных условий, воспользуйтесь функцией регистрации.

Некоторые публикации по iSeries содержат примеры программ выхода, предназначенных для защиты системы. Список примеров программ выхода с указанием источника, в котором они опубликованы, приведен в Табл. 24.

Таблица 24. Исходный код примеров программ выхода

Тип программы выхода	Назначение	Где можно найти примеры
Проверка пароля	Имя этой программы хранится в системном значении QIBM_QSY_VLD_PASSWRD. Она проверяет новый пароль на соответствие дополнительным требованиям, которые не учитываются всеми остальными системными значениями QPWDxxx. Следует тщательно проверить алгоритм работы этой программы, так как она получает пароли в незашифрованном виде. Эта программа **не должна** сохранять пароли в файле или передавать их другим программам.	• *An Implementation Guide for iSeries Security and Auditing, GG24–4200* • *iSeries Security Reference*, SC41-5302-07
Доступ через PC Support/400 или Client Access[1]	Имя этой программы указывается в параметре Обработка запросов клиента (PCSACC) сетевых атрибутов. Она управляет следующими функциями: • Функцию виртуального принтера • Функцию передачи файлов • Функцию общих папок типа 2 • Функцию сообщений Client Access • Функцию очередей данных • Функцию удаленного SQL	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Доступ к Управлению распределенными данными (DDM)	Имя этой программы указывается в параметре обработки запросов к DDM (DDMACC) сетевых атрибутов. Она управляет следующими функциями: • Общими папками типов 0 и 1 • Функцией запуска удаленной команды	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Удаленный вход в систему	Имя этой программы указывается в системном значении QRMTSIGN. Она проверяет, что данному пользователю указанного компьютера разрешен удаленный вход в систему.	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*

Таблица 24. Исходный код примеров программ выхода (продолжение)

Тип программы выхода	Назначение	Где можно найти примеры
Обращение к ODBC через iSeries Access[1]	Управляет следующими функциями ODBC: • Разрешено ли применение ODBC. • Какие функции работы с файлами базы данных iSeries разрешено применять. • Какие операторы SQL разрешено применять. • Какую информацию об объектах сервера базы данных разрешено предоставлять. • Какие функции работы с каталогом SQL разрешено применять.	Примеров нет.
Программа обработки прерывания QSYSMSG	В зависимости от типа сообщения, помещенного в очередь QSYSMSG, эта программа выполняет определенное действие (например, уведомляет администратора защиты).	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
TCP/IP	В некоторых серверах TCP/IP (например, FTP, TFTP, TELNET, и REXEC) предусмотрены точки выхода. Вы можете создать программу выхода для обработки входа пользователя в систему или проверки пользовательских запросов, например, запросов на получение или запись файла. Кроме того, с помощью этих точек выхода вы можете настроить в системе FTP с анонимным доступом.	"Раздел TCP/IP User Exits книги *iSeries System API Reference*"
Изменение пользовательского профайла	Вы можете создать программы выхода, вызываемые при выполнении следующих команд для работы с пользовательскими профайлами: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries Security Reference*, SC41-5302-07 • "Раздел TCP/IP User Exits книги *iSeries System API Reference*"

Примечания:

1. Дополнительная информация по этому разделу приведена в iSeries Information Center. Подробные сведения приведены в разделе "Необходимая и полезная информация" на стр. xii.

Глава 16. Рекомендации по настройке защиты в Web-браузерах

Наверняка на многих персональных компьютерах в вашей организации установлены браузеры. Они предназначены для подключения к Internet, и, в частности, к серверу. Ниже приведены некоторые советы по организации защиты PC и сервера:

Возможная опасность: повреждение данных на рабочей станции

С любой Web-страницей, открытой пользователем, может быть связана программа, например, аплет Java, управляющий элемент Active-X или другой встраиваемый модуль. Возможно, хотя и маловероятно, что в результате запуска этой программы на PC будут повреждены его информационные ресурсы. В связи с этим администратор защиты должен предпринять следующие действия для защиты PC в своей организации:

- Ознакомьтесь с функциями защиты, предусмотренными в тех браузерах, которые применяются вашими пользователями. Например, некоторые браузеры позволяют ограничить доступ аплетов Java к ресурсам локальной системы (такая среда выполнения Java называется *средой с ограниченными возможностями*). Эта опция позволяет запретить аплетам изменять данные PC.

  Примечание: Среда с ограниченными возможностями и связанные с ней функции защиты неприменимы для Active-X и других встраиваемых модулей.
- Сообщите пользователям, какую конфигурацию браузера рекомендуется выбрать. Скорее всего, у вас не будет времени и возможности убедиться, что все пользователи выполнили ваши рекомендации. В связи с этим рекомендуется заранее проинформировать пользователей о возможных последствиях отклонения от рекомендуемых значений.
- Рекомендуется установить на всех компьютерах одинаковые Web-браузеры, предоставляющие необходимые функции защиты.
- Порекомендуйте пользователям информировать вас обо всех подозрительных с точки зрения защиты Web-сайтах.

Возможная опасность: доступ к каталогам iSeries через сетевые диски

Предположим, что PC подключился к серверу, установив сеанс IBM iSeries Access для Windows. При установке сеанса настраиваются сетевые диски, необходимые для обращения к интегрированной файловой системе iSeries. Например, диск **G** персонального компьютера может быть подключен к интегрированной файловой системе сервера SYSTEM1.

Предположим, что этот PC подключен к Internet и на нем установлен браузер. Пользователь этого компьютера может открыть Web-страницу, запускающую опасную программу, например, аплет Java или управляющий элемент Active-X. Эта программа потенциально может удалить все данные с диска G персонального компьютера.

Существует несколько способов защиты сетевых дисков:

- Самая надежный способ защиты - это защита ресурсов на сервере. С точки зрения сервера аплет Java или управляющий элемент Active-X ничем не отличается от

пользователя PC, установившего сеанс. Следовательно, нужно четко определить, какие права доступа должны быть предоставлены пользователям PC.

- Посоветуйте пользователям PC запретить в конфигурации браузера доступ к сетевым дискам. Это позволит защитить сетевые диски от аплетов Java, но не от управляющих элементов Active-X, для которых нельзя создать среду выполнения с ограниченными возможностями.
- Проинформируйте пользователей о возможных последствиях одновременного подключения к серверу и Internet. Кроме того, напомните пользователям PC (например, с операционной системой Windows 95), что сетевые диски остаются подключенными даже после завершения сеанса iSeries Access.

Возможная опасность: подписанные аплеты

Предположим, что все пользователи выполнили вашу рекомендацию и запретили аплетам записывать данные на диски PC, выбрав соответствующую опцию в параметрах браузера. В этом случае необходимо учесть то, что *подписанный аплет* может переопределить эту опцию браузера.

Для идентификации такого аплета с ним связана цифровая подпись. Когда пользователь открывает Web-страницу с подписанным аплетом, ему отправляется сообщение. Это сообщение содержит подпись аплета (информацию о том, кем и когда был подписан этот аплет). При получении аплета пользователь предоставляет ему права на переопределение параметров защиты браузера. Подписанный аплет может записывать информацию на локальные диски PC, даже если это запрещено соответствующей опцией браузера. Такой аплет может записывать информацию и на диски сервера, подключенные к PC в качестве локальных дисков.

Вы можете разрешить применение подписанных аплетов Java, загружаемых с локального сервера. Однако следует проинформировать пользователей о том, что в общем случае не рекомендуется принимать подписанные аплеты, загруженные с внешнего сервера.

Глава 17. Дополнительная информация

Руководства

- *APPC Programming*, SC41-5443-00 содержит информацию о поддержке расширенных средств межпрограммной связи (APPC) для системы iSeries. В ней приведены инструкции по разработке прикладных программ с применением APPC и по определению среды для средств связи APPC. Рассмотрены основные правила создания прикладных программ, требования к конфигурации, команды, действия по устранению неполадок для APPC и общие принципы работы с сетями. Электронную версию этой книги можно найти на компакт-диске с iSeries Information Center.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet*, SG24-4929, содержит сведения о различных вопросах защиты, в том числе о возможных негативных последствиях подключения системы iSeries к сети Internet. В ней приведены примеры, рекомендации, советы и технологии, применяемые для приложений TCP/IP.
- *Backup and Recovery*, SC41-5304-07 содержит описание вопросов планирования стратегии резервного копирования и восстановления, а также процедур сохранения и восстановления информации в системе. Электронную версию этой книги можно найти в iSeries Information Center. Дополнительная информация по этим темам приведена в iSeries Information Center. Дополнительная информация приведена в разделе “Необходимая и полезная информация” на стр. xii.
- *CL Programming*, SC41-5721-06 содержит подробное описание процедур создания спецификаций описания данных (DDS) для файлов, допускающих внешнее описание. Эти файлы могут быть физическими, логическими, файлами дисплея, принтера или файлами межсистемной связи (ICF). Электронную версию этой книги можно найти в iSeries Information Center.
- В разделе CL справочной системы Information Center (дополнительная информация приведена в разделе “Необходимая и полезная информация” на стр. xii) приведено описание синтаксиса языка CL системы iSeries и команд CL операционной системы OS/400. Команды OS/400 применяются для вызова функций лицензионной программы Operating System/400 (5722-SS1). Команды CL, относящиеся к другим лицензионным программам, в том числе команды изменения поддержки языка и различные утилиты, описаны в книгах по соответствующим лицензионным программам.
- *Implementing iSeries Security, 3rd Edition* by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press, отдел Duke Communications International, 1998. Здесь приведены инструкции и практические советы по планированию, настройке и управлению защитой iSeries.

  Номер заказа ISBN:

  1-882419-78-2
- Дополнительная информация о сервере HTTP приведена на следующем Web-сайте:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Security Reference*, SC41-5302-07 содержит полную информацию о системных значениях защиты, пользовательских профайлах, защите ресурсов и контроле защиты. Это руководство не рассматривает защиту отдельных лицензионных программ, языков и утилит. Электронную версию этой книги можно найти в iSeries Information Center.

- В разделе ″Работа с системой″ документации Information Center приведена общая информация о работе с системой iSeries и описаны основные задачи. Подробная информация приведена в “Необходимая и полезная информация” на стр. xii.
- В Information Center можно найти информацию о настройке и применении TCP/IP и различных приложений TCP/IP, в том числе FTP, SMTP и TELNET. Дополнительная информация приведена в разделе “Необходимая и полезная информация” на стр. xii.
- В книге *TCP/IP File Server Support for OS/400 Installation and User's Guide*, SC41-0125, приведена обзорная информация, инструкции по установке и процедуры настройки лицензионной программы File Server Support. В ней описаны функции этого продукта и приведены примеры и советы по его применению в других системах.
- В книге *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, описаны критерии уровней надежности компьютерных систем. TCSEC - это публикация правительства Соединенных Штатов. Ее копии можно получить по адресу:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- Information Center содержит ряд разделов, посвященных управлению системой iSeries и ее заданиями. В частности, приведена информация о сборе статистических данных, изменении системных значений и управлении памятью системы. Подробные инструкции по работе с Information Center приведены в разделе “Необходимая и полезная информация” на стр. xii. Книга Work Management, SC41-5306-03, содержит информацию о создании и изменении стратегии управления заданиями. Электронную версию этой книги можно найти в iSeries Information Center.

Помимо описанных руководств и разделов Information Center, существуют следующие источники информации:

- **IBM SecureWay**
  IBM SecureWay - это общее название целого набора средств защиты, предлагаемых UBM, включающего аппаратного и программное обеспечение, справочные системы и службы, предназначенные для тех заказчиков, которые хотят защитить свои информационные ресурсы. IBM SecureWay предлагает средства планирования, разработки, реализации и внедрения систем защиты как для отдельных пользователей, так и для больших компаний. Дополнительная информация о продуктах IBM SecureWay приведена на домашней странице IBM SecureWay:
  `http://www.ibm.com/secureway`
- **Услуги**
  Установка нового аппаратного и программного обеспечения позволяет значительно повысить эффективность работы. В то же время она влечет за собой опасность возникновения сбоя и последующего простоя системы или повреждения важных внутренних ресурсов. Служба IBM Global Services предоставляет различные услуги, связанные с организацией защиты системы iSeries. Полную информацию обо всех услугах, относящихся к системе iSeries, можно найти на следующем Web-сайте:
  `http://www.as.ibm.com/asus`

Примечания

Настоящая информация предназначена для продуктов и услуг, распространяемых в США.

IBM может не предоставлять продукты, программы и услуги, упоминаемые в этом документе, в других странах. Информацию о продуктах и услугах, распространяемых в вашей стране, можно получить в местном представительстве IBM. Ссылки на продукты, программы или услуги фирмы IBM не означают, что можно использовать только указанные продукты, программы или услуги IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако ответственность за проверку пригодности и применение таких программ, продуктов и услуг несет пользователь.

IBM может располагать патентами или заявками на получение патента по отношению к материалам, упоминаемым в настоящем документе. Предоставление настоящего документа не означает, что вместе с ним вы получаете какие-либо лицензии на эти патенты. Запросы на лицензии можно направлять в письменном виде по адресу:

IBM
Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Запросы на лицензии, связанные с обработкой информации DBCS (набор двухбайтовых символов), следует направлять в местное представительство IBM Intellectual Property Department или в письменном виде по адресу:

IBM
World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Следующий абзац не относится к Великобритании, а также к 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.

Эта публикация может содержать технические неточности или типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. Фирма IBM оставляет за собой право в любое время и без дополнительного уведомления вносить исправления и улучшения в продукты и программы, упоминаемые в настоящей публикации.

Любые ссылки на Web-сайты, не принадлежащие фирме IBM, приведены здесь исключительно для удобства и никоим образом не означают, что фирма IBM обслуживает эти сайты или несет ответственность за их содержание. Информация, приведенная на этих Web-сайтах, не является частью документации по данному продукту. Фирма IBM не несет ответственности за работу этих Web-сайтов.

IBM оставляет за собой право использовать или распространять любую предоставленную вами информацию теми способами, которыми сочтет нужным, без возникновения каких-либо обязательств перед вами.

Лицам, обладающим лицензией на эту программу и желающим получить о ней информацию с целью: (i) осуществлять обмен информацией между независимо создаваемыми программами и другими программами (включая данную); и (ii) совместно использовать информацию, полученную в результате обмена, следует обратиться по следующему адресу:

IBM
Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Эти сведения предоставляются на определенных условиях, включающих в некоторых случаях дополнительную оплату.

Лицензионная программа, рассматриваемая в настоящей публикации, и все связанные с ней лицензионные материалы предоставляются фирмой IBM на условиях Договора об Обслуживании Заказчиков фирмы IBM, Международного Соглашения о Лицензии на Программу фирмы IBM или любого эквивалентного договора.

Все данные о производительности, приведенные в настоящей публикации, были определены при работе в управляемой среде. По этой причине результаты, полученные в другой операционной среде, могут отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на стадии разработки, поэтому нет гарантии, что эти измерения дадут те же результаты в обычных системах. Более того, некоторые значения были определены путем экстраполяции. Фактические значения могут быть другими. Пользователям, работающим с настоящим документом, следует проверить данные в конкретной среде.

Информация о продуктах, поставляемых не фирмой IBM, была получена от поставщиков этих продуктов, из опубликованных этими поставщиками заявлений или из других общедоступных источников. Фирма IBM не проводила тестирование этих продуктов и не может гарантировать указанную производительность этих продуктов, их совместимость с продуктами фирмы IBM и другие заявленные характеристики. Вопросы, касающиеся продуктов, поставляемых не фирмой IBM, следует направлять поставщикам этих продуктов.

Все заявления о будущих действиях или намерениях фирмы IBM могут быть изменены или аннулированы без дополнительного уведомления; такие заявления следует рассматривать только как информацию о предполагаемых целях и задачах фирмы IBM.

Следующая информация предназначена исключительно для целей планирования. Приведенная информация может измениться до того, как описанные продукты станут доступны.

Настоящая информация содержит примеры данных и отчетов, применяемых в повседневных деловых операциях. Для большей достоверности в примерах указаны имена людей, названия компаний, товарные знаки и названия продуктов. Все эти имена вымышленные; любое их возможное совпадение с реальными именами и адресами является случайным.

Лицензия на продукты, защищенные авторским правом:

В настоящей документации приведены примеры исходных текстов прикладных программ, иллюстрирующие некоторые приемы программирования в различных операционных платформах. Разрешается бесплатно копировать, изменять и распространять в любой форме эти примеры с целью разработки, использования и распространения прикладных программ для интерфейсов, соответствующих той операционной платформе, для которой созданы примеры. Указанные примеры не были тщательно и всесторонне протестированы. По этой причине, фирма IBM не может гарантировать их надежность и пригодность. Фирма IBM разрешает бесплатно копировать, изменять и распространять в любой форме эти примеры с целью разработки, использования и распространения прикладных программ, предназначенных для интерфейсов прикладных программ фирмы IBM.

В электронной версии настоящей информации могут отсутствовать фотографии и цветные изображения.

Товарные знаки

Следующие названия являются товарными знаками фирмы International Business Machines Corporation в США, других странах или и в тех, и в других:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (логотип)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium и ProShare - это зарегистрированные товарные знаки Intel Corporation в США и/или других странах.

Microsoft, Windows, Windows NT и логотип Windows - это товарные знаки Microsoft Corporation в США и/или других странах.

Java, а также все товарные знаки, включающие слово Java, - это товарные знаки Sun Microsystems, Inc. в США и/или других странах.

UNIX - зарегистрированный в США и других странах товарный знак The Open Group.

Названия других фирм, продуктов и услуг могут быть товарными и сервисными знаками соответствующих фирм.

Индекс

Спец. символы

A

B

C

D

E

R

S

Г

Д

Ж

З

И

К

Л

М

Н

О

П

P

C

Т

У

Ф

Х

Ц

Ч

Ш

Э

Отзывы читателей

iSeries
Рекомендации по защите сервера iSeries
Версия 5

Номер публикации SC43-0125-07

Мы ждем ваших отзывов об этой публикации. Не стесняйтесь указать на то, что вы считаете ошибками или недостатками, а также оценить точность, структуру изложения, соответствие теме и полноту информации в данной книге. Просим касаться в ваших замечаниях только материала, представленного в данной книге, и способа его изложения.

По техническим вопросам и для получения информации по продуктам IBM и ценам на них обращайтесь к представителю фирмы IBM, бизнес-партнерам IBM или к авторизованному поставщику продукции IBM.

По общим вопросам звоните +7(095)9402000.

Отсылая информацию фирме IBM, вы тем самым предоставляете IBM неисключительное право использовать или распространять эту информацию так, как фирма сочтет нужным, без каких-либо обязательств с ее стороны.

Комментарии:

Благодарим за сотрудничество.

Чтобы представить ваши комментарии:
- Пошлите ваши комментарии по адресу, указанному на обратной стороне этой формы.
- Пошлите факс по следующему номеру: Для США и Канады: 1-800-937-3430
- Пошлите ваши комментарии по электронной почте на адрес: RCHCLERK@us.ibm.com

Если вы хотите получить ответ от IBM, пожалуйста, укажите следующую информацию:

Имя	Адрес
Компания или Организация	
Номер телефона	Адрес e-mail

Отзывы читателей
SC43-0125-07

IBM

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 Highway 52 N
ROCHESTER MN

Напечатано в Дании

SC43-0125-07