ООО «ИБМ Восточная Европа/Азия»

СОГЛАСОВАНО
Начальник
2 Управления ФСТЭК РОССИИ

В.В. СЕЛИН
«7» июля 2008 года

УТВЕРЖДАЮ
Директор департамента
программного обеспечения
ООО «ИБМ Восточная Европа/Азия»

Л.Г. АЛТУХОВ
«04» 07 2008 года

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ IBM LOTUS DOMINO ENTERPRISE SERVER AND NOTES FOR MULTIPLATFORMS V. 7.0.2.

ЗАДАНИЕ ПО БЕЗОПАСНОСТИ

IBM.LOTUS_DOMINO/NOTES7_0_2_ENT.3Б

Версия 1.0

Москва, 2008 г.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

ЗБ	– задание по безопасности
ИТ	– информационная технология
ОДФ	– область действия функции безопасности объекта оценки
ОК	– Общие критерии
ОО	– объект оценки (Administrator Client, Designer Client, Notes, Domino Server)
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
ПФБ	– политика функции безопасности
СФБ	– стойкость функции безопасности
УК	– управление конфигурацией
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональные требования безопасности

1 ВВЕДЕНИЕ ЗБ

Данный раздел содержит информацию общего характера. Подраздел «Идентификация ЗБ» предоставляет идентификационную и описательную информацию, необходимую, чтобы идентифицировать, каталогизировать ЗБ и ссылаться на него. Подраздел «Аннотация ЗБ» содержит общую характеристику ЗБ в форме пригодной для размещения в виде самостоятельного реферата в каталогах ЗБ. В подразделе «Соглашения» дается описание правил обозначения результатов выполнения операций конкретизации компонентов требований безопасности ИТ. В подразделе «Термины и определения» представлены определения основных терминов, используемых в настоящем ЗБ. В подразделе «Организация ЗБ» дается пояснение организации настоящего ЗБ.

1.1 Идентификация ЗБ

Название ЗБ:	Программное обеспечение IBM Lotus Domino Enterprise Server and Notes for multiplatforms v. 7.0.2. Задание по безопасности.
Версия ЗБ:	Версия 1.0.
Обозначение ЗБ:	IBM.LOTUS_DOMINO/NOTES7_0_2_ENT.ЗБ
Идентификация ОО:	Программное обеспечение IBM Lotus Domino Enterprise Server and Notes for multiplatforms v. 7.0.2.
Уровень доверия:	ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности).
Идентификация ОК:	ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». ГОСТ Р ИСО/МЭК 15408-2-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности» ГОСТ Р ИСО/МЭК 15408-3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности». Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1, 2, 3», Гостехкомиссия России, 2002.

Ключевые слова: средство защиты информации, дискреционное управление доступом, задание по безопасности, ОУД1, IBM.

1.2 Аннотация ЗБ

Настоящее ЗБ определяет требования безопасности для программного обеспечения IBM Lotus Domino Enterprise Server and Notes for multiplatforms v.7.0.2.

Объект оценки (ОО) представляет собой ИТ-систему, предназначенную для коллективной работы, обеспечивающую надежную инфраструктурную платформу высокой производительности.

1.3 Соглашения

Руководящий документ Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – Общие критерии) допускает выполнение определенных в части 2 ОК операций над функциональными требованиями. Соответственно в настоящем ЗБ используются операции «уточнение», «выбор», «назначение» и «итерация».

Операция **«уточнение»** используется для добавления к требованию некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей его удовлетворения. Результат операции **«уточнение»** в настоящем ЗБ обозначается **полужирным текстом**.

Операция **«выбор»** используется для выбора одного или нескольких элементов из перечня в формулировке требования. Результат операции **«выбор»** в настоящем ЗБ обозначается *подчеркнутым курсивным текстом*.

Операция **«назначение»** используется для присвоения конкретного значения ранее неконкретизированному параметру. Операция **«назначение»** обозначается заключением значения параметра в квадратные скобки, [назначаемое значение].

Операция **«итерация»** используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении разрешенных операций (уточнение, выбор, назначение). Выполнение «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

Замечания по применению предназначены либо для разъяснения назначения некоторого требования, идентификации вариантов реализации, либо для определения

условий выполнения требования. В случае использования, замечания по применению следуют за компонентом требования.

В настоящее ЗБ включены компоненты функциональных требований безопасности, сформулированные в явном виде. Краткая форма имен функциональных компонентов, сформулированных в явном виде, содержит текст (EXT).

1.4 Термины и определения

В настоящем ЗБ применяются следующие термины с соответствующими определениями.

Активы – информация или ресурсы ОО, подлежащие защите контрмерами ОО.

Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора.

Аутентификация – процесс установления подлинности информации, предъявленной администратором ОО и пользователем ОО при регистрации.

Достоверность – свойство безопасности активов, обеспечивающее соответствие предусмотренным значениям.

Зависимость – соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть удовлетворено, чтобы и другие требования могли отвечать своим целям.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО (в данном случае – ПО IBM Lotus Domino Enterprise Server and Notes for multiplatforms v. 7.0.2.).

Идентификатор – уникальный признак администратора ОО или пользователя ОО, однозначно его идентифицирующий.

Конфиденциальность – свойство безопасности активов предотвращать возможность доступа к информации и/или ее раскрытия неуполномоченным лицам, объектам или процессам.

Объект ОО – сущность в пределах ОДФ, которая содержит или получает информацию, и над которой субъекты выполняют операции.

Объект оценки – подлежащая оценке ПО IBM Lotus Domino Enterprise Server and Notes for multiplatforms v. 7.0.2. с руководствами по эксплуатации.

Подконтрольность – свойство безопасности активов, обеспечивающее однозначное отслеживание действий объектов и субъектов информационных отношений.

Политика безопасности ОО – совокупность правил, регулирующих управление, защиту и распределение активов, контролируемых ОО.

Политика функции безопасности – политика безопасности, осуществляемая ФБ.

Пользователь – любая сущность (человек-пользователь или внешний объект ИТ) вне ОО, которая взаимодействует с ОО.

Администратор ОО – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию ОО.

Продукт ИТ – совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы (в данном случае продукт ИТ совпадает с ОО, идентифицированным в настоящем ЗБ).

Профиль защиты – независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

Ресурс ОО – все, что может использоваться или потребляться в ОО (вычислительные возможности, физическая память, дисковое пространство).

Система ИТ – специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Субъект ОО – сущность в пределах ОДФ, которая инициирует выполнение операций (процессы, действующие от имени пользователей ОО).

Функции безопасности ОО – совокупность всех функций безопасности ОО, направленных на осуществление ПБО.

Функция безопасности – функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

Целостность – свойство безопасности активов, обеспечивающее поддержание полноты и неизменности информации.

1.5 Организация ЗБ

Задание по безопасности включает следующие разделы: «Введение ЗБ», «Описание ОО», «Среда безопасности ОО», «Требования безопасности ИТ», «Утверждения о соответствии ПЗ» и «Обоснование».

Раздел 1 «Введение ЗБ» содержит информацию, в которой идентифицируется ЗБ и изделие ИТ (включая номер версии) и дается аннотация ЗБ для включения в список оцененных (сертифицированных) изделий ИТ.

Раздел 2 «Описание ОО» содержит описание функциональных возможностей ОО, среды функционирования ОО и границ ОО, служащее цели лучшего понимания требований безопасности и дающее представление о типе системы ИТ.

Раздел 3 «Среда безопасности ОО» содержит описание аспектов среды безопасности ОО (проблему безопасности, которую необходимо решить). В данном разделе определяется совокупность угроз, которым должен противостоять ОО, правила политики безопасности, которой должен следовать ОО, и предположения (обязательные условия) безопасного использования ОО.

В разделе 4 «Цели безопасности» определена совокупность целей безопасности для ОО и среды функционирования ОО. Цели безопасности отражают сформулированное предназначение ЗБ. Они раскрывают, каким образом ОО должен противостоять идентифицированным угрозам и учитывать предположения и политику безопасности организации.

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 ОК определены, соответственно, функциональные требования безопасности ИТ, включая требования к стойкости функций безопасности ОО, реализуемым вероятностными или перестановочными механизмами, и требования доверия к безопасности ОО.

В Разделе 6 «Краткая спецификация ОО» содержит описание функций безопасности ИТ, реализуемых изделием ИТ и соответствующих специфицированным функциональным требованиям безопасности, а также мер доверия к безопасности, соответствующих специфицированным требованиям доверия к безопасности.

В Разделе 7 «Утверждения о соответствии ПЗ» содержит описание соответствия данного ЗБ какому-либо ПЗ.

В Разделе 8 «Обоснование» демонстрируется, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает идентифицированные аспекты среды безопасности ОО.

2 ОПИСАНИЕ ОО

Объектом оценки в настоящем ЗБ является ПО для организации совместной работы IBM Lotus Domino Enterprise Server and Notes for multiplatforms v. 7.0.2.

2.1 Тип продукта ИТ

Объект оценки (ОО) представляет собой ИТ-систему (IBM Lotus Domino Enterprise Server and Notes for multiplatforms v. 7.0.2.), предназначенную для коллективной работы, обеспечивающую надежную инфраструктурную платформу высокой производительности. В ее состав входит Administrator Client, Notes Client, Designer Client, Notes, Domino.

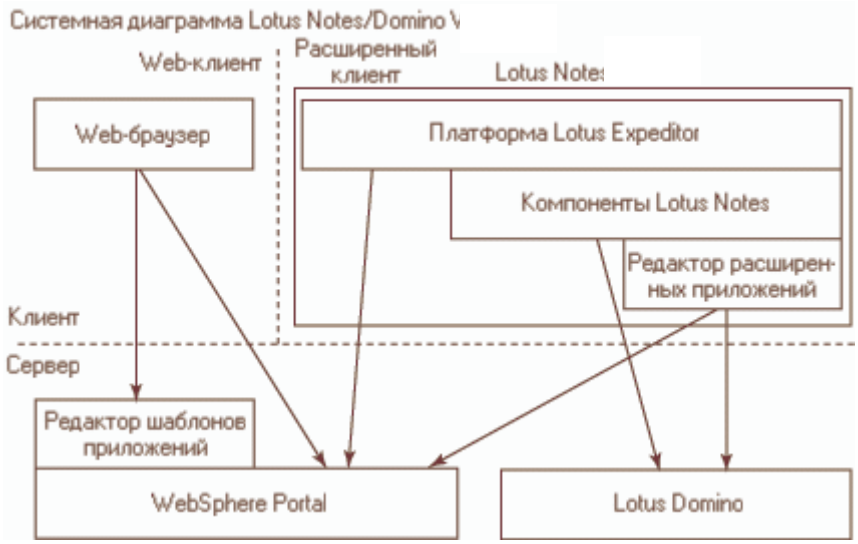

Рис.1 Структура ПО IBM Lotus Notes/Domino

На рисунке показаны компоненты ОО и взаимодействие между ними.

Web-браузер может использовать составное приложение только через WebSphere Portal, однако в Lotus Notes входит вся функциональность, необходимая для работы с составными приложениями.

2.2 Основные функциональные возможности ОО

В ОО реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность ИТ, надежность ПО, а также упрощающих администрирование ОО и управление вычислительной средой ОО. В данном подразделе представлено краткое описание этих функциональных возможностей и средств.

2.2.1 Основные функциональные возможности обеспечения безопасности

ПО характеризуется как управляемая, надежная и безопасная система, что достигается за счет таких возможностей обеспечения безопасности, как использование единых регистрационных данных пользователя при доступе к ОС и к ПО, аудит событий безопасности, управление ролями, дискреционное управление доступом.

2.2.1.1 Аудит событий безопасности

ОО обеспечивает широкие возможности, связанные с мониторингом и обнаружением нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в вычислительной среде. Мониторинг относящихся к безопасности событий позволяет обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к ПО или доступа к защищаемым активам. В частности, определяя политику аудита, уполномоченный администратор ОО может осуществлять аудит только необходимых классов событий безопасности, таких как создание и удаление пользователей ПО или неудачные попытки подключения пользователей к базе данных. Запись результатов аудита событий безопасности осуществляется в журналы регистрации событий аудита, доступ к которому разрешен только уполномоченному администратору ОО.

2.2.1.2 Дискреционное управление доступом

В ОО доступ к защищаемым активам разрешен только уполномоченным на это пользователям ОО. Модель защиты ОО включает компоненты, которые реализуют контроль субъектов доступа и действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый пользователь, осуществляющий взаимодействие с ПО, представлен в ней регистрационной записью, определяющей сущностей, имеющих право доступа к БД, и учетной записью пользователя БД, сопоставленной с регистрационной записью и используемой платформой при управлении доступом как к самой БД (базам данных), так и ее объектам. Для каждой БД система поддерживает собственный список дискреционного управления доступом, в которой определены права доступа к объектам данной БД. Список дискреционного управления доступом включает перечень пользователей и ролей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

2.2.1.3 Управление учетными данными пользователей ОО

Функция управления учетными данными обеспечивает безопасное хранение учетных данных пользователя БД. ПО поддерживает список, в котором полностью определены учетные записи пользователей, имеющих доступ к БД. При этом список учетных записей пользователей поддерживается отдельно для каждой существующей БД, для которой определены права доступа. Если пользователю необходимо получить доступ к какой-либо БД, то при осуществлении попыток доступа к ней потребуется пройти процедуру проверки подлинности, в ходе которой пользователь предъявляет свой идентификатор безопасности, на основании которого определяется возможность доступа пользователя к данной БД.

2.2.1.4 Управление ролями

Использование ролей позволяет упростить управление доступом к защищаемым активам, позволяя назначать разрешения и права группе пользователей, а не отдельной учетной записи. Таким образом, исходя из потребностей в доступе к новым активам, пользователь ОО может быть включен в состав участников определенной роли или исключен из участия в указанной роли.

ПО поддерживает ряд предопределенных ролей сервера БД, создаваемых в момент установки. Членство в данных ролях предоставляет право выполнять ряд административных и системных задач, такие как управление файлами и устройствами резервного копирования, установка и изменение параметров конфигурации удаленных и связанных серверов БД и т.д.

2.2.2 Основные функциональные возможности повышения надежности

ПО обеспечивает надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

2.2.2.1 Резервное копирование данных

В ПО входят стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования предоставляют пользователям возможность выбора различных стратегий резервного копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы.

2.2.2.2 Возможности масштабирования

ПО обеспечивает функции масштабирования для развертывания и поддержки больших производственных баз и хранилищ данных, а также для создания отказоустойчивых кластеров.

2.2.3 Основные средства администрирования, управления и поддержки

Средства администрирования, управления и поддержки обеспечивают полномасштабное и гибкое управление ПО.

2.2.4 Основные функциональные возможности обеспечения сетевой безопасности

ПО обеспечивает возможность поддержки безопасных сетей, построенных на основе протокола SSL.

Поддержка протокола SSL обеспечивает передачу функций проверки подлинности осуществляющих доступ к БД пользователей ОС, под управлением которой функционирует ПО.

2.3 Среда функционирования и границы ОО

2.3.1 Среда функционирования

Среда функционирования ОО определяется вариантами установки клиентских приложений и ОО и предусматривает установку приложений и ОО либо на одном компьютере, либо на разных компьютерах, объединенных в сеть. Функционирование ОО предполагается под управлением следующих серверных ОС: 32-bit Microsoft Windows Server 2003 Entrerprise Edition; 64-bit Sun Solaris 9; 64-bit AIX v5.3; 64-bit Su Se Linux Enterprise Server 9 with SP2; 64-bit Red Hat Linux v4.

2.3.2 Логические границы ОО

Объект оценки представляет собой модульную систему, состоящую из нескольких программных компонентов, совместно решающих различные задачи. Каждый компонент ОО имеет необходимые интерфейсы для взаимодействия с другими компонентами системы.

2.3.3 Физические границы ОО

Физические границы ОО включают персональный компьютер (сервер) со следующими минимально необходимыми аппаратными характеристиками (см. таблицу 2.1).

Таблица 2.1.

№ п/п	Показатель	Минимальные требования	Рекомендуемые требования
1.	Процессор	тактовая частота процессор Intel Pentium III или аналогичный 1 ГГц	тактовая частота процессор Intel Pentium III или аналогичный 1,4 ГГц и более
2.	Объем оперативной памяти	512 Мб	1024 Мб и более
3.	Привод CD-ROM	привод CD- или DVD-ROM из списка совместимого оборудования HCL	
4.	Монитор	SVGA-совместимый, обеспечивающий поддержку разрешения экрана не менее 1024x768 точек.	
5.	Объем свободного дискового пространства	Не менее 2 Гб свободного места	

2.4 Службы безопасности ОО

В данном подразделе приводится краткое описание служб безопасности ОО, реализующих оцениваемые (в соответствии с настоящим ЗБ) функции безопасности ОО.

2.4.1 Аудит безопасности

Объект оценки обеспечивает распознавание, запись и хранение информации, связанной с событиями, существенными с точки зрения безопасности. Категории событий, подлежащих регистрации, определяются администратором ОО и могут детализироваться вплоть до конкретного класса событий. После настройки параметров политики аудита можно отслеживать всю совокупность относящихся к безопасности событий аудита и анализировать недостатки системы безопасности. Записи аудита, содержащие сведения о выбранных событиях, включают информацию о пользователе, который был инициатором события и выполнял какие-либо действия в отношении контролируемого объекта доступа. ОО обеспечивает возможность доступа к журналу аудита только уполномоченным на это администраторам ОО.

2.4.2 Защита данных пользователя

Объект оценки осуществляет функции и политику дискреционного (избирательного) управления доступом. Дискреционное управление доступом

предоставляет возможность ограничивать и контролировать доступ к ОО, базам данных, схемам и их объектам. Каждый пользователь, пытающийся получить доступ к ОО, сначала проходит аутентификацию, а затем, при попытках получения доступа к ресурсам – авторизацию, т.е. проверку разрешений пользователя по отношению к какому-либо защищаемому объекту.

2.4.3 Идентификация и аутентификация

Идентификация и аутентификация пользователя должны осуществляться до выполнения им каких-либо действий в ОО.

Механизм идентификации предполагает наличие у пользователя его уникального регистрационного имени (ID) и генерации уникального ключа.

В специальном файле-идентификаторе, который может храниться только у пользователя на носителе, содержаться все необходимые пользователю данные: его полное имя, пароль, сертификаты, общий (публичный) и личный ключ, специальные ключи шифрования, номер лицензии.

Процесс установления подлинности (процедура аутентификации) включает четыре этапа:

1. Установление сервером доверия к публичному ключу клиента (станции, другого сервера).

Когда клиент пытается установить связь с сервером, содержащиеся в ID-файле клиента имя и публичный ключ посылаются на сервер. Клиент по запросу сервера также присылает список сертификатов, которые будут использоваться, чтобы подтвердить ассоциацию между именем клиента и его публичным ключом. Присланные клиентом сертификаты необходимо проверить, для выполнения этой проверки нужен публичный ключ выдавшего "присланный" сертификат сертификатора. Получить этот ключ следует из более заслуживающего доверия источника, чем "присланный" клиентом сертификат или "своя" общая адресная книга.

2. Проверка, знает ли клиент свой личный ключ:

-сервер генерирует случайное число и посылает его клиенту;

-клиент шифрует это число своим личным ключом и возвращает полученный код серверу;

-сервер использует публичный ключ клиента для декодирования присланного клиентом кода.

Сервер предполагает, что клиент подлинный только в том случае, если декодированное число совпадает с оригиналом.

3. Установление клиентом доверия к публичному ключу сервера.

Процесс "зеркально аналогичен" рассмотренному выше процессу установления сервером доверия публичному ключу клиента. В случае использования взаимных сертификатов этот процесс завершается успешно только тогда, когда в локальной адресной книге клиента имеется взаимный сертификат, выпущенный клиентом или одним из предков клиента для сервера или одного из предков сервера.

4. Проверка клиентом, знает ли сервер свой личный ключ – "зеркально" повторяет процесс проверки сервером факта знания клиентом своего личного ключа.

Ведется список разрешенных пользователей для входа в систему, который может быть изменен администратором безопасности. Не пройдя процедуры идентификации, невозможно загрузить профиль пользователя.

2.4.4 Управление безопасностью

Объект оценки осуществляет функции, обеспечивающие управление ролями, а также предоставляющие ряд возможностей по управлению различными характеристиками безопасности. Использование ролей обеспечивает простой механизм назначения полномочий пользователю на выполнение определенных действий в БД и над ее объектами. ОО поддерживает ряд предопределенных ролей сервера БД, создаваемых в момент установки, и фиксированные роли БД, для которых определены предопределенные полномочия для работы с БД.

2.4.5 Защита ФБО

Объект оценки и среда функционирования ОО предоставляют ряд возможностей для обеспечения защиты функций безопасности ОО, таких как обеспечение целостности ФБО, поддержание домена безопасности и предоставление ФБО надежных меток времени.

2.4.6 Управление доступом к ОО

Объект оценки обеспечивает возможность ограничения открытия сеанса доступа на основе идентификатора регистрационной записи пользователя. При обращении пользователя к ОО, ФБО осуществляют проверку разрешений на подключение данного субъекта доступа. Проверка осуществляется на основе идентификатора регистрационной

записи пользователя, для которого администратором определены разрешающие или запрещающие права доступа к ОО.

2.4.7 Использование ресурсов ОО

В ОО предусмотрены механизмы управления размером БД, предоставляющие возможность ограничивать объем доступного для БД дискового пространства.

Устанавливаемый по умолчанию для файлов данных и файлов журналов транзакций минимальный размер равен 64 Mb, максимальный размер файлов неограничен. Чтобы контролировать рост файлов БД и объем свободного дискового пространства, ОО предоставляет возможность ограничивать объем доступного для БД дискового пространства, что исключает неограниченное увеличение ее размера. Уполномоченному администратору предоставлена возможность управления минимальным и максимальным размером, величиной приращения и параметром автоматического увеличения размера для каждого файла данных.

3 ОПИСАНИЕ ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

– предположений относительно предопределенного использования ОО и аспектов безопасности среды ОО;

– угроз безопасности, которым нужно противостоять средствами ОО;

– политики безопасности организации, которой должен следовать ОО.

3.1 Предположения безопасности

3.1.1 Предположения относительно предопределенного использования ОО

A.ImpossibleModif

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

A.Connect

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

A.Peer

Должно быть обеспечено взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

A.TOEConfig

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

A.OSAuth

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

A.Environment

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от

прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

A.RecoverySafeState

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

A.Locate

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположения, имеющее отношение к персоналу

A.NoEvilAdm

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

A.NoEvilUser

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

3.2Угрозы

3.2.1 Угрозы, которым противостоит ОО

В настоящем ЗБ определены следующие угрозы, которым противостоит ОО.

T.UnauthAccessData

1. Аннотация угрозы – осуществление доступа к информации, размещаемой на объектах ОО, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к информации, размещаемой на объектах ОО, с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к объектам ОО, связанные с возможностью предоставления доступа к информации, размещаемой на объектах ОО, неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – информация, размещаемая на объектах ОО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, размещаемой на объектах ОО; несанкционированная модификация информации (в том числе подмена), размещаемой на объектах ОО; несанкционированное удаление информации, размещаемой на объектах ОО.

T.UnauthExecProc&Fanc

1. Аннотация угрозы – выполнение хранимых процедур и определяемых функций неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к хранимым процедурам и определяемым функциям с использованием приложений, поддерживающих возможность взаимодействия с ОО, и запуск их на выполнение.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к объектам ОО, связанные с возможностью выполнения хранимых процедур и определяемых функций неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – хранимые процедуры и определяемые функции.

6. Нарушаемое свойство безопасности активов – несанкционированное выполнение.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, выдаваемой после отработки хранимых процедур и функций; нарушение режимов функционирования ОО и БД.

T.UnauthAccessTOE

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся в БД.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией, хранящейся в БД.

T.MasqAdmin&User

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией, хранящейся в БД; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

T.UnauthAccessAuditData

1. Аннотация угрозы – осуществление доступа к данным аудита ОО пользователями ОО и неуполномоченными на это администраторами ОО и возможность несанкционированного удаления и модификации данных аудита ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способы реализации угрозы – осуществление доступа к данным аудита ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным аудита с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к данным аудита, связанные с возможностью осуществления доступа к данным аудита пользователями ОО и неуполномоченными на это администраторами ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – подконтрольность, целостность, конфиденциальность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля действий пользователей ОО и администраторов ОО, а также контроля процесса функционирования ОО в целом; навязывание администраторам ОО, ответственным за контроль данных аудита ОО, ложных (модифицированных) данных аудита; несанкционированное ознакомление о произошедших в ОО событиях.

T.LostAuditDataOverStg

1. Аннотация угрозы – потеря данных аудита ОО вследствие переполнения выделенного для задач аудита хранилища информации.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – переполнение выделенного для задач аудита хранилища информации.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за переполнения хранилища данных аудита ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

T.LostAuditDataOverDisk

1. Аннотация угрозы – потеря данных аудита ОО вследствие исчерпания свободного дискового пространства.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – исчерпание свободного дискового пространства.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за исчерпания свободного дискового пространства.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

T.UnauthAccessTSF

1. Аннотация угрозы – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным ФБО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

T.UnauthUsageRes

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на это субъектами.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

3.2.2 Предположения относительно предопределенного использования ОО

В настоящем ЗБ определены следующие угрозы, которым противостоит среда функционирования ОО.

TE.UnauthAccessTOE

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся в БД.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией.

TE.MasqAdmin&User

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

TE.UnauthAccessTSF

1. Аннотация угрозы – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным ФБО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

TE.UnauthUsageRes

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на использование субъектами в нарушение политики безопасности.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

TE.UnauthAccessData

1. Аннотация угрозы – осуществление доступа к информации ОО, хранимой на уровне ОС в файлах файловой системы, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к информации, хранимой в файлах, с использованием приложений, поддерживающих возможность осуществления доступа к файлам.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к файлам, связанные с возможностью предоставления доступа к информации, размещаемой в файлах, неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – информация, хранимая в файлах.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, хранимой в файлах; несанкционированная модификация информации (в том числе подмена), хранимой в файлах; несанкционированное удаление информации, хранимой в файлах.

3.3Политика безопасности организации

Объект оценки должен следовать приведенным ниже правилам политики безопасности организации.

P.Manage

Должны быть в наличии надлежащие корректно функционирующие средства администрирования ОО, доступные только уполномоченным администраторам ОО.

P.Audit

Должны быть обеспечены надлежащая регистрация и предупреждение администратора ОО о любых событиях, относящихся к безопасности ОО. Должна быть обеспечена возможность для администратора ОО выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

P.Resourse

Для уполномоченного администратора ОО должна быть обеспечена возможность управления надлежащим распределением ресурсов ОО.

P.Access

Должна быть обеспечена возможность для уполномоченных на это пользователей ОО определять доступность объектов ОО для других пользователей ОО.

P.GenerateTime

Должна быть обеспечена привязка по времени событий, подвергаемых аудиту.

P.TOEAuth

Должна обеспечиваться аутентификация субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности, механизмами самого ОО.

P.ManageAuthData

В случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, операционная система должна предоставлять механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

4 ЦЕЛИ БЕЗОПАСНОСТИ

4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

O.AccessObject

Разграничение доступа к объектам ОО

ОО должен обеспечивать доступ к объектам ОО только уполномоченным на это пользователям ОО. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО определять доступность объектов ОО для других пользователей ОО.

O.AccessTOE

Разграничение доступа к ОО

ОО должен обеспечивать доступ к ОО только уполномоченным на это пользователям.

O.TOEAuth

Аутентификация с использованием механизмов ОО

ОО должен обеспечивать аутентификацию субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности.

O.AuditEvents

Аудит событий

ОО должен располагать надлежащими механизмами регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации должны предоставлять администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

O.ProtectAudit

Защита данных аудита

ОО должен обеспечивать доступ к данным аудита только уполномоченным администраторам ОО и предотвращать потерю данных аудита в случае переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

O.AdminManage

Наличие средств администрирования

ОО должен располагать надлежащими корректно функционирующими средствами администрирования, доступными только уполномоченным администраторам ОО.

O.ProtectResTSF

Защита данных ФБО и ресурсов ОО

ОО должен обеспечивать защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

O.DistrResourse

Распределение ресурсов ОО

ОО должен обеспечивать для уполномоченного администратора ОО возможность надлежащего распределения ресурсов ОО.

4.2 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для среды функционирования ОО.

OE.ImpossibleModif

Замкнутость среды функционирования

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

OE.Connect

Контролируемые точки доступа

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.Peer

Взаимодействие с доверенными системами

Должно быть обеспечено взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

OE.TOEConfig

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

OE.OSAuth

Аутентификация с использованием механизмов ОС

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

OE.Environment

Стойкость функции безопасности

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.ManageAuthData

Управление качеством аутентификационных данных

В случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, операционная система должна предоставлять механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.Locate

Физическая защита ОО

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.NoEvilAdm

Требования к администраторам ОО

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

OE.NoEvilUser

Требования к пользователям ОО

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

OE.ProtectResTSF

Защита данных ФБО и ресурсов ОО

Должна быть обеспечена защита данных ФБО и ресурсов ОО, а также поддержка домена для функционирования ФБО.

OE.GenerateTime

Поддержка аудита

Должна быть обеспечена поддержка средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

OE.ProtectFileSystem

Защита на уровне файловой системы

Должна быть обеспечена защита данных, размещаемых в базах данных ОО, на уровне файлов файловой системы ОС от несанкционированного доступа.

OE.RecoverySafeState

Восстановление ОО

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

5 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ

В данном разделе ЗБ представлены требования безопасности ИТ, которым должен удовлетворять ОО и его среда. Функциональные требования, представленные в настоящем ЗБ, основаны на функциональных компонентах из части 2 ОК. Требования доверия основаны на компонентах требований доверия из части 3 ОК и представлены в настоящем ЗБ в виде оценочного уровня доверия ОУД1, усиленного компонентом доверия AVA_SOF.1 (Оценка стойкости функции безопасности ОО).

5.1 Требования безопасности для ОО

5.1.1 Функциональные требования безопасности ОО

Функция безопасности «Аутентификация» реализуется механизмом паролей. Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости. В качестве минимального уровня стойкости функции безопасности «Аутентификация» в настоящем ЗБ заявлена «Средняя СФБ» Другие механизмы (некриптографические), реализуемые ФБО, нельзя отнести к вероятностным и перестановочным механизмам, поэтому заявлений об их стойкости в настоящем ЗБ не делается.

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности ОО, приведены в таблице 5.1.

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF. 1	Управление доступом, основанное на атрибутах безопасности
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.2	Идентификация до любых действий пользователя

Идентификатор компонента требований	Название компонента требований
FIA_USB.1	Связывание пользователь – субъект
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_REV.1	Отмена
FMT_SMR.1	Роли безопасности
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FRU_RSA.2	Минимальные и максимальные квоты
FTA_TSE.1	Открытие сеанса с ОО

5.1.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на *неопределенном* уровне аудита;

в) (события, приведенные во втором столбце таблицы 5.2).

FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

а) дата и время события, тип события, идентификатор субъекта и результат

события (успешный или неуспешный);

б) для каждого типа событий, потенциально подвергаемых аудиту, из

числа определенных в функциональных компонентах, которые включены в ЗБ, [информацию, определенную в третьем столбце таблицы 5.2].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во	

Компонент	Событие	Детализация
	время сбора данных аудита.	
FAU_STG.3	Предпринимаемые действия после превышения порога заполнения журнала аудита	
FAU_STG.4	Факт останова ОО при отсутствии свободного дискового пространства для создания журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на именованном объекте, на который распространяется политика дискреционного управления доступом	
FIA_AFL.1 (1)	Достижение ограничения неуспешных попыток аутентификации и предпринятые действия	
FIA_UAU.2 (1)	Все случаи использования механизма аутентификации субъектов доступа	
FIA_UID.2	Все случаи использования механизма идентификации субъектов доступа	
FIA_USB.1	Факт создания регистрационной и учетной записи пользователя	
FMT_MOF.1	Все модификации режима выполнения аудита и режима аутентификации	
FMT_MSA.1	Все модификации значений атрибутов безопасности, используемых в политике дискреционного управления доступом	
FMT_MSA.3	Модификации настройки по умолчанию ограничительных правил, все модификации начальных значений атрибутов безопасности, которые используются для политики дискреционного управления доступом	
FMT_MTD.1	Все модификации значений данных ФБО	
FMT_REV.1 (1)	Все попытки отмены полномочий у пользователей ОО на доступ к объектам, отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_REV.1 (2)	Все попытки отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_SMR.1	Модификация множества администраторов ОО и пользователей ОО	
FTA_TSE.1	Все попытки открытия сеанса доступа к ОО со стороны субъектов	
FRU_RSA.2 (1)	Установление и модификация объема физической памяти, доступного для ОО	
FRU_RSA.2 (2)	Установление и модификация объема дискового пространства для баз данных	

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором **учетной записи** пользователя **или идентификатором регистрационной записи пользователя,** который был инициатором этого события.

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FIA_UID.2 «Идентификация до любых действий пользователя».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченному администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** воспринимать содержащуюся в них информацию.

Зависимости: FAU_GEN.1 «Генерация данных аудита».

FAU_SAR.2 Ограниченный просмотр аудита

FAU_SAR.2.1 ФБО должны запретить всем пользователям доступ к чтению записей аудита, за исключением **уполномоченных администраторов ОО**, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны **предоставить** возможность выполнить поиск данных аудита, основанный на

[

следующих критериях в логическом отношении «И»:

а) наименование поля данных;

б) значение поля данных

].

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:

а) ***категория*** *события;*

[

б) класс события;

в) поле данных

].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 «Управление данными ФБО».

FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.1.1 ФБО должны защищать хранимые записи аудита от несанкционированного удаления.

FAU_STG.1.2 ФБО должны быть способны к предотвращению модификации записей аудита.

Зависимости: FAU_GEN.1 «Генерация данных аудита».

FAU_STG.3 Действия в случае возможной потери данных аудита

FAU_STG.3.1 ФБО должны выполнить [создание нового журнала аудита], если журнал аудита **превысит** [установленный уполномоченным администратором ОО размер].

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны выполнить *игнорирование событий, подвергающихся аудиту* и [останов ОО] при **отсутствии свободного дискового пространства для создания журнала аудита.**

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

5.1.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] для

[

а) субъектов – процессов, действующих от имени пользователей;

б) именованных объектов:

1) на уровне сервера БД – конечная точка (Endpoint), регистрационная запись (Login), база данных (Database);

2) на уровне БД – схема (Schema), пользователь (Database User), роль (Role), полнотекстовый каталог (Full Text Catalog);

3) на уровне схемы – функция (Function), представление (Views), очередь (Query), типы (Types), коллекция XML-схем (XML Schema Collection);

в) всех операций между субъектами и объектами

].

Зависимости: FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] к объектам, основываясь на

[

следующем:

а) ассоциированные с субъектом идентификатор учетной записи пользователя, принадлежность к роли (ролям), определяемой пользователем;

б) следующие, ассоциированные с объектами, атрибуты управления

доступом:

[

– владелец объекта;

– список дискреционного управления доступом, который сопоставлен с объектом доступа и содержит записи:

– идентификатор учетной записи пользователя или роли, определяемой пользователем;

– тип (разрешение или запрет);

– право доступа к объекту;

]

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

доступ к объекту разрешен, если, по крайней мере, выполняется одно из следующих условий:

а) субъект является владельцем объекта;

б) запись, содержащаяся в списке дискреционного управления доступом, явно разрешает доступ субъекту, и доступ не был явно запрещен записью, содержащейся в списке дискреционного управления доступом;

в) запись, содержащаяся в списке дискреционного управления доступом, явно разрешает доступ роли, участником которой является субъект, и доступ не был явно запрещен записью, содержащейся в списке дискреционного управления доступом;

в случае если доступ к объекту не разрешен правилами, изложенными в FDP_ACF.1.3, то доступ субъекта к объекту запрещен

].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах:

[

а) уполномоченному администратору ОО предоставлен доступ к объектам ОО вне зависимости от списков дискреционного управления доступом

б) полномочия администратора ОО на доступ к объекту определяются

участием в предопределенных ролях сервера БД (server role) и (или) фиксированных ролях БД (fixed database role), предполагающих возможность доступа к объектам вне зависимости от списков дискреционного управления доступом

].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах:

[

в доступе к объекту явно отказано, если выполняется, по крайней мере, одно из следующих условий:

а) запись в списке дискреционного управления доступом явно запрещает доступ для субъекта;

б) запись в списке дискреционного управления доступом явно запрещает доступ роли, участником которой является субъект

].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_MSA.3 «Инициализация статических атрибутов».

5.1.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 (1) Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [установленное администратором ОО число (не более 10)] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного в элементе **FIA_AFL.1.1** числа неуспешных попыток аутентификации ФБО должны:

[

а) сделать невозможным доступ субъекта доступа к ОО, осуществив блокировку регистрационной записи;

б) осуществить сброс счетчика неуспешных попыток аутентификации

по команде уполномоченного администратора ОО

].

Зависимости: FIA_UAU.2 (1) «Аутентификация до любых действий пользователя».

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

[

а) идентификатор регистрационной записи пользователя;

б) идентификатор роли, участником которой является пользователь;

в) идентификатор учетной записи пользователя

].

Зависимости: отсутствуют.

FIA_UAU.2 (1) Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый **субъект доступа к ОО и объектам ОО** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого субъекта доступа.

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый **субъект доступа к ОО и объектам ОО** был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого субъекта доступа.

Зависимости: отсутствуют.

FIA_USB.1 Связывание пользователь-субъект

FIA_USB.1.1 ФБО должны ассоциировать соответствующие атрибуты безопасности **субъекта доступа** с субъектами, действующими от имени этого **субъекта доступа.**

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

5.1.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность *определять режим выполнения, модифицировать режим выполнения* функций, связанных с:

[

а) аудитом;

б) аутентификацией субъектов доступа

]

только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность *модифицировать*

атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** *ограничительные* значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом.

FMT_MSA.3.2 ФБО должны позволять [уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта.

Зависимости: FMT_MSA.1 «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность [*выполнения операций*] над данными, только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с ***пользователями ОО и объектами***, в пределах ОДФ только [уполномоченному администратору ОО].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

а) отмена полномочий у пользователей ОО на доступ к объектам должна вступать в силу при следующем сеансе работы пользователя ОО;

б) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с ***объектами***, в пределах ОДФ только [пользователю ОО, являющемуся владельцем объекта].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

а) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[

а) администратор ОО;

б) пользователь ОО

].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать субъектов доступа с ролями.

Зависимости: FIA_UID.2 «Выбор момента идентификации».

5.1.1.5 Защита ФБО (FPT)

FPT_RVM.1 (1) Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 (1) Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

5.1.1.6 Использование ресурсов (FRU)

FRU_RSA.2 (1) Минимальные и максимальные квоты

FRU_RSA.2.1 ФБО должны реализовать максимальные квоты [объема физической памяти], который ***ОО*** может использовать ***в процессе функционирования.***

FRU_RSA.2.2 ФБО должны обеспечить выделение минимального [объема физической памяти], который является доступными для ***ОО***, чтобы использовать ***в процессе функционирования.***

Зависимости: отсутствуют.

FRU_RSA.2 (2) Минимальные и максимальные квоты

FRU_RSA.2.1 ФБО должны реализовать максимальные квоты [объема дискового пространства], который базы данных могут использовать одновременно.

FRU_RSA.2.2 ФБО должны обеспечить выделение минимального [объема дискового пространства], который является доступными для баз данных, чтобы использовать одновременно.

Зависимости: отсутствуют.

5.1.1.7 Доступ к ОО (FTA)

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса доступа к ОО, основываясь на

[

следующих атрибутах:

а) идентификатор регистрационной записи пользователя;

б) предельное количество одновременно открытых сеансов доступа к

ОО

].

Зависимости: отсутствуют.

5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 ОК и образуют ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности ОО) (см. таблицу 5.3).

Таблица 5.3 – Требования доверия к безопасности ОО

Класс доверия	Идентификатор компонентов доверия	Название компонентов доверия
Управление конфигурацией	ACM_CAP.1	Номера версий
Поставка и эксплуатация	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_RCR.1	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО

5.1.2.1 Управление конфигурацией (ACM)

ACM_CAP.1 Номера версий

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

ACM_CAP.1.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

ACM_CAP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.2 Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

ADO_IGS.1.1D Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

Элементы содержания и представления свидетельств

ADO_IGS.1.1C Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.

Элементы действий оценщика

ADO_IGS.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1.2E Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

5.1.2.3 Разработка (ADV)

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_FSP.1.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.1.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.1.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

ADV_FSP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.1.2E Оценщик должен сделать независимое заключение, что функциональная спецификация – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_RCR.1.1D Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

ADV_RCR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.4 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

AGD_ADM.1.1D Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования.

Элементы содержания и представления свидетельств

AGD_ADM.1.1C Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.

AGD_ADM.1.2C Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.

AGD_ADM.1.3C Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_ADM.1.4C Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.

AGD_ADM.1.5C Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.

AGD_ADM.1.6C Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.

AGD_ADM.1.7C Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_ADM.1.8C Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.

Элементы действий оценщика

AGD_ADM.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

AGD_USR.1.1C Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.

AGD_USR.1.2C Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.

AGD_USR.1.3C Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_USR.1.4C Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.

AGD_USR.1.5C Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_USR.1.6C Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.

Элементы действий оценщика

AGD_USR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.5 Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ATE_IND.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.1.2E Оценщик должен протестировать необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

5.1.2.6 Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

AVA_SOF.1.1D Разработчик должен выполнить анализ стойкости функции безопасности ОО для каждого механизма, идентифицированного в ЗБ как имеющего утверждение относительно стойкости функции безопасности ОО.

Элементы содержания и представления свидетельств

AVA_SOF.1.1C Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.

AVA_SOF.1.2C Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ/ЗБ.

Элементы действий оценщика

AVA_SOF.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.2Требования безопасности для среды ИТ

Функцией безопасности, реализуемой средой ИТ (операционной системой) в интересах обеспечения безопасности ОО, является функция безопасности «Аутентификация». Данная функция реализуется механизмом паролей среды ИТ (операционной системы). Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости. В качестве минимального уровня стойкости функции безопасности «Аутентификация» в настоящем ЗБ заявлена «**Средняя СФБ**».

Другие механизмы (некриптографические), реализуемые средой ИТ в интересах обеспечения безопасности ОО, нельзя отнести к вероятностным и перестановочным механизмам, поэтому заявлений об их стойкости в настоящем ЗБ не делается.

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.4.

Таблица 5.4 – Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FIA_AFL.1	Обработка отказов аутентификации
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени

5.2.1 Идентификация и аутентификация (FIA)

FIA_AFL.1 (2) Обработка отказов аутентификации

FIA_AFL.1.1 **Функции безопасности среды ИТ** должны обнаруживать, когда произойдет [установленное администратором ОС число (не более 10)] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного **в элементе FIA_AFL.1.1** числа неуспешных попыток аутентификации **функции безопасности среды ИТ** должны:

[

а) сделать невозможным доступ субъекта доступа к ОО, осуществив блокировку регистрационной записи на 30 минут;

б) по истечении 30 минут осуществить сброс счетчика неуспешных попыток аутентификации

].

Зависимости: FIA_UAU.2 (2) «Аутентификация до любых действий пользователя».

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 **Функции безопасности среды ИТ** должны предоставить механизм для верификации того, что **пароли на доступ к ОО** отвечают **следующей метрики качества**

[

а) минимальная длина – 6 символов;

б) пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

в) в пароле должны присутствовать символы как минимум трех категорий из числа следующих:

– прописные буквы английского алфавита от A до Z;

– строчные буквы английского алфавита от a до z;

– десятичные цифры от 0 до 9;

– символы, не принадлежащие алфавитно-цифровому набору;

].

Зависимости: отсутствуют.

FIA_UAU.2 (2) Аутентификация до любых действий пользователя

FIA_UAU.2.1 Функции безопасности среды ИТ должны требовать, чтобы каждый субъект доступа к ОО и объектам ОО был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого субъекта доступа.

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

5.2.2 Защита ФБО (FPT)

FPT_RVM.1 (2) Невозможность обхода ПБО

FPT_RVM.1.1 Функции безопасности среды ИТ должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 (2) Отделение домена ФБО

FPT_SEP.1.1 Функции безопасности среды ИТ должны поддерживать домен безопасности для выполнения ФБО, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 Функции безопасности среды ИТ должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 Функции безопасности среды ИТ должны быть способны предоставить надежные метки времени для использования ФБО.

Зависимости: отсутствуют.

6 КРАТКАЯ СПЕЦИФИКАЦИЯ ОО

В данном подразделе представлено описание функций безопасности ОО и мер доверия к безопасности ОО, а также – их сопоставление с требованиями безопасности для ОО.

6.1 Функции безопасности ОО

6.1.1 Управление доступом

ФБО ОО должны обеспечивать пользователям возможность получения доступа, основанного на идентификаторе пользователя/группы и связи(ях) с ролью, только к следующим ресурсам:

- Web-модулям;
- Определениям портлетного приложения;
- Базам данных;
- Узлам содержимого (Страницам);
- Группам пользователей;
- URL, отображающим контексты.

Для обращения к ресурсам используется Web-браузер. Пользователь идентифицируется в среде ОО. Идентификаторы пользователя и группы поддерживаются в рамках среды. Связи с ролями поддерживаются *Admin*, *Security_Admin* через административное приложение *Разрешения Группы пользователей* и *Разрешения Ресурса*. ОО предоставляет доступ к ресурсу только, если идентификатор пользователя (или группы, к которой принадлежит идентификатор пользователя) связан с соответствующими ролями, которые в свою очередь связаны с ресурсом.

Роли создаются посредством связей наборов действий с ресурсами. Права доступа сохраняются в БД. Доступ к дочерним ресурсам может быть запрещен блокированием роли. Это – либо блокирование распространения, которое запрещает наследование управления доступом, распространяющееся к дочерним ресурсам, либо блокирование наследования, которое предотвращает наследование управления доступом от этого ресурса соответственно. Решение от ОО

возвращается соответствующему клиенту как булево да/нет. Если доступ разрешен, то клиент ОО выполняет требуемую операцию, и результаты возвращаются пользовательскому интерфейсу. Если в доступе отказано, то, в зависимости от требуемой операции, либо отсутствует отображение ресурса на клиенте ОО, либо выдается ошибка.

6.1.2 Определение значений атрибутов, заданных по умолчанию

Начальные параметры настройки управления доступом приведены в таблице 6.1.

Таблица 6.1 – Начальные параметры настройки

Пользователь или группа	Роль
Административный пользователь, идентифицированный во время инсталляции	*Administrator*
<admins>	*Administrator*
Все аутентифицированные пользователи	*User@* следующие портлетные приложения: • Редактировать содержание и размещение страницы • Конкретные Свойства Сетевых Приложений • Добро пожаловать • Вид сетевого приложения • Портлеты установки разрешений • Информационное портлетное приложение • Свойства страницы • Организованные предпочтения • Персонализатор страниц *Privileged_User@* следующие страницы: • Мой портал

admins - группа пользователей, которая устанавливается по умолчанию при инсталляции ОО. Пользователь обладает действиями, связанными с ролью: User, Editor и Privileged_User. Никакого явного назначения роли для этих действий нет. Они являются частью политики администрирования.

При создании ресурса ФБО должны определять значения по умолчанию атрибутов безопасности для доступа к этому ресурсу. Всякий раз, когда защищаемый ресурс создается в рамках портала, пользователь, создавший ресурс, становится владельцем этого ресурса. Владельцу ресурса разрешается выполнять следующие действия на ресурсе:

- добавлять дочерний (если ресурс является общедоступным);
- добавлять частный дочерний (если ресурс является частным);

- удалять;
- редактировать (если ресурс является общедоступным);
- персонализировать (если ресурс является частным);
- просматривать.

Кроме того, ресурс наследует разрешения, назначенные на родительский ресурс, если на месте нет блокирования распространения. Частными являются ресурсы, к которым можно обратиться только владельцам этого ресурса. Следовательно, действие «Добавлять частный дочерний ресурс» дает возможность создания дочернего ресурса, к которому разрешается иметь доступ только владельцу. Персонализировать – это то же самое разрешение, что и редактировать, но для частного ресурса. Общедоступные ресурсы – это ресурсы, к которым можно обращаться более чем одному пользователю.

6.1.3 Администрирование управлением доступа

Роли *Administrator* и *Security_Administrator* содержат разрешение (*Предоставлять доступ к (виртуальному ресурсу) порталу)*, которое недоступно для любой другой роли. Это разрешение позволяет Администратору или Администратору Безопасности делать произвольные изменения в конфигурации управления доступом всех ресурсов, которые управляются внутри ОО. Администратор и Администратор Безопасности могут просматривать, создавать и удалять роли, назначения ролей и блокирования наследования.

Администрирование управления доступом может производиться в выполняющемся приложении при помощи соответствующих программных интерфейсов сценариев *XmlAccess*. Выполнение сценария XmlAccess требует действий (Предоставлять Доступ к (виртуальному ресурсу) порталу) и (Предоставлять Доступ к (виртуальному ресурсу) XmlAccess).

ОО поддерживает передачу административных полномочий по управлению доступом. Администратор – это пользователь, который уполномочен изменять конфигурацию управления доступом, переназначая роли и создавая или удаляя блокирования ролей. Администраторы могут передавать определенные подмножества их

административных привилегий другим пользователям или группам. Эти пользователи или группы, в свою очередь, могут передавать подмножества их привилегий другим пользователям и группам.

6.1.4 Действия

Действия обеспечиваются как часть набора. Следующие действия доступны:

- Действие «Предоставлять доступ к» поддерживает деятельность по предоставлению или отмене другим участникам разрешений на доступ к конфигурации управления доступом на определенном ресурсе;
- Действие «Передавать полномочия для» поддерживает деятельность по передаче разрешений определенному участнику.;
- Действие «Добавлять дочерний ресурс» поддерживает создание нового, общедоступного ресурса ниже существующего ресурса;
- Действие «Добавлять частный дочерний ресурс» поддерживает создание нового частного ресурса ниже существующего ресурса, к которому можно обратиться только одному пользователю;
- Действие «Удалять» поддерживает удаление ресурса или отсоединение ресурса от его родительского ресурса (например, когда ресурс перемещается из одного места в топологии в другое);
- Действие «Редактировать» поддерживает все модификации ресурса (например, изменение метаинформации ресурса), которые видимы не только владельцу ресурса;
- Действие «Персонализировать» поддерживает все модификации ресурса, которые являются видимыми только владельцу ресурса (под этим может подразумеваться неявное создание производного ресурса);
- Действие «Просматривать» поддерживает предъявление содержания или метаинформации ресурса.

Действия – это часть «набора действий». Наборы действий характеризуют определенные типы ролей, которые могут из них создаваться. Чтобы обеспечивать безопасное функционирование ОО, ФБО должны поддерживать наборы действий, приведенные в таблице 6.2. Эти действия устанавливаются в ОО по умолчанию и не могут быть отредактированы.

Таблица 6.2 – Наборы действий, характеризующие типы ролей

Действия	Наборы Действий						
	Администратор	**Администратор безопасности**	**Передающий полномочия**	**Менеджер**	**Редактор**	**Привилегированный пользователь**	**Пользователь**
Предоставлять доступ к	x	x					
Передавать полномочия для	x	x	x				
Добавлять Дочерний	x			x	x		
Добавлять Частный Дочерний	x					x	
Удалять	x			x			
Редактировать	x			x	x		
Персонализировать	x					x	
Просматривать	x			x	x	x	x

6.2 Меры доверия к безопасности ОО

Для удовлетворения требований доверия к безопасности согласно ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), применены следующие меры доверия к безопасности ОО:

– управление конфигурацией;
– предоставление руководств;
– предоставление проектной документации;
– тестирование;
– оценка стойкости функций безопасности.

6.2.1 Управление конфигурацией

Меры управления конфигурацией, применяемые корпорацией IBM, обеспечивают уникальную идентификацию версий ОО.

Корпорация IBM осуществляет уникальную маркировку ОО, позволяющую отличать разные версии ОО. Это достигается маркированием упаковки, носителей. Кроме того, ОО может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку или графический интерфейс.

Сопоставление с ТДБ

Меры доверия, связанные с управлением конфигурацией, удовлетворяют следующему требованию доверия:

– ACM_CAP.1.

6.2.2 Предоставление руководств

Корпорация IBM предоставляет руководства безопасной установки, генерации и запуска. В процедурах установки, генерации и запуска описаны шаги, необходимые для получения безопасной конфигурации ОО, описанной в ЗБ.

Корпорация IBM предоставляет руководства администратора и пользователя, в которых описываются действия по выполнению функций безопасности ОО и приводятся предупреждения уполномоченным администраторам и пользователям о действиях, которые могут скомпрометировать безопасность ОО.

Сопоставление с ТДБ

Меры доверия, связанные с представлением руководств, удовлетворяют следующим требованиям доверия:

– ADO_IGS.1;

– AGD_ADM.1;

– AGD_USR.1.

6.2.3 Представление проектной документации

Проектная документация ОО, предоставляемая на оценку, включает функциональную спецификацию. Функциональная спецификация является неформальной.

В функциональной спецификации определены все внешние (то есть, видимые для пользователя или администратора) интерфейсы функций безопасности ОО, описаны режимы функционирования ОО на каждом внешнем интерфейсе, включая описание результатов, нештатных ситуаций и сообщений об ошибках.

Материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией направлены на отображения соответствия функций безопасности, представленных в функциональной спецификации, функциям безопасности, идентифицированным в краткой спецификации.

Сопоставление с ТДБ

Меры доверия, связанные с представлением проектной документации, удовлетворяют следующим требованиям доверия:

– ADV_FSP.1;

– ADV_RCR.1.

6.2.4 Тестирование

Корпорация IBM предоставляет ОО, пригодный для тестирования, с соответствующей документацией, это позволяет провести независимое тестирование ФБО и сделать заключение, выполняются ли ФБО в соответствии со спецификациями.

Сопоставление с ТДБ

Меры доверия, связанные с тестированием, удовлетворяют требованию доверия:

– ATE_IND.1.

6.2.5 Оценка стойкости функции безопасности

В ОО отсутствуют функции, которые характеризуются стойкостью, поэтому анализ стойкости функций не производится.

7 УТВЕРЖДЕНИЯ О СООТВЕТСТВИИ ПЗ

Соответствие данного ЗБ какому-либо профилю защиты не декларируется.

8 ОБОСНОВАНИЕ

В данном разделе дано обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ЗБ. В разделе «Обоснование» также демонстрируется справедливость утверждений о СФБ и соответствии ПЗ.

8.1 Обоснование целей безопасности

8.1.1 Оценка стойкости функции безопасности

В таблице 8.1 приведено отображение целей безопасности для ОО на угрозы и политику безопасности организации.

Таблица 8.1 – Отображение целей безопасности на угрозы и политику безопасности организации

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
T.UnauthAccessData	X							
T.UnauthExecProc&Fanc	X							
T.UnauthAccessTOE		X						
T.MasqAdmin&User		X						
T.UnauthAccessAuditData					X			
T.LostAuditDataOverStg					X			
T.LostAuditDataOverDisk					X			
T.UnauthAccessTSF							X	
T.UnauthUsageRes							X	
P.Manage						X		
P.Audit				X				
P.Resourse								X
P.Access	X							

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
P.TOEAuth			**X**					

O.AccessObject

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessData, T.UnauthExecProc&Fanc** и реализацией политики безопасности организации **P.Access,** так как обеспечивает доступ к объектам ОО только уполномоченным пользователям ОО, а также обеспечивает возможность уполномоченным пользователям ОО определять доступность объектов ОО для других пользователей ОО.

O.AccessTOE

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessTOE и T.MasqAdmin&User**, так как обеспечивает доступ к ОО только уполномоченным на это пользователям.

O.TOEAuth

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.TOEAuth**, так как обеспечивает аутентификацию субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности.

O.AuditEvents

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Audit**, так как обеспечивает наличие надлежащих механизмов регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации предоставляют администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

O.ProtectAudit

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessAuditData, T.LostAuditDataOverStg и T.LostAuditDataOverDisk**, так как обеспечивает доступ к данным аудита только уполномоченным администраторам

ОО и предотвращает потерю данных аудита в случае переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

O.AdminManage

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Manage,** так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования, доступных только уполномоченным администраторам ОО.

O.ProtectResTSF

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessTSF и T.UnauthUsageRes**, так как обеспечивает защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

O.DistrResourse

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Resourse**, так как обеспечивает для уполномоченного администратора ОО возможность надлежащего распределения ресурсов ОО.

8.1.2 Обоснование целей безопасности для среды

В таблице 8.2 приведено отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности организации.

Таблица 8.2 – Отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности организации

	OE.ImpossibleModif	OE.Connect	OE.Peer	OE.TOEConfig	OE.OSAuth	OE.Environment	OE.ManageAuthData	OE.Locate	OE.NoEvilAdm	OE.NoEvilUser	OE.ProtectResTSF	OE.GenerateTime	OE.ProtectFileSystem	OE.RecoverySafeState
A.ImpossibleModif	X													
A.Connect		X												
A.Peer			X											
A.TOEConfig				X										

	OE.ImpossibleModif	OE.Connect	OE.Peer	OE.TOEConfig	OE.OSAuth	OE.Environment	OE.ManageAuthData	OE.Locate	OE.NoEvilAdm	OE.NoEvilUser	OE.ProtectResTSF	OE.GenerateTime	OE.ProtectFileSystem	OE.RecoverySafeState
A.OSAuth					X									
A.Environment						X								
A.RecoverySafeState														X
A.Locate								X						
A.NoEvilAdm									X					
A.NoEvilUser										X				
TE.UnauthAccessTOE					X									
TE.MasqAdmin&User					X									
TE.UnauthAccessTSF											X			
TE.UnauthUsageRes											X			
TE.UnauthAccessData													X	
P.GenerateTime												X		
P.ManageAuthData							X							

OE.ImpossibleModif

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.ImpossibleModif**, так как обеспечивает отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

OE.Connect

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Connect**, так как обеспечивает осуществление доступа к ОО только из санкционированных точек доступа, размещенных в контролируемой зоне, т.е. охраняемой территории и помещении, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.Peer

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Peer**, так как обеспечивает взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

OE.TOEConfig

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.TOEConfig**, так как обеспечивает установку конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

OE.OSAuth

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.OSAuth** и противостояния угрозам **TE.UnauthAccessTOE** и **TE.MasqAdmin&User**, так как обеспечивает осуществление аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов ОС, под управлением которой функционирует ОО.

OE.Environment

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Environment**, так как обеспечивает осуществление функционирования ОО в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.ManageAuthData

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.ManageAuthData**, так как в случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, обеспечивает предоставление операционной системой механизмов управления качеством аутентификационных данных, обеспечивающих адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.Locate

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Locate**, так как обеспечивает, для предотвращения несанкционированного физического доступа, размещение компьютера с установленным

ОО в контролируемой зоне, т.е. охраняемой территории и помещении, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.NoEvilAdm

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.NoEvilAdm**, так как обеспечивает прохождение персоналом, ответственным за администрирование ОО, проверок на благонадежность и компетентность, а также деятельность согласно соответствующей документации.

OE.NoEvilUser

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.NoEvilUser**, так как обеспечивает прохождение уполномоченными на доступ к ОО пользователями проверок на благонадежность, а их совместные действия, направлены исключительно на выполнение своих функциональных обязанностей.

OE.ProtectResTSF

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **TE.UnauthAccessTSF и TE.UnauthUsageRes**, так как обеспечивает защиту данных ФБО и ресурсов ОО, а также поддержку домена для функционирования ФБО.

OE.GenerateTime

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.GenerateTime**, так как обеспечивает поддержку средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

OE.ProtectFileSystem

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **TE.UnauthAccessData**, так как обеспечивает защиту данных, размещаемых в БД, на уровне файлов файловой системы ОС от несанкционированного доступа.

OE.RecoverySafeState

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.RecoverySafeState**, так как обеспечивает выполнение мероприятий, направленных на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

8.2 Обоснование требований безопасности

8.2.1 Обоснование требований безопасности для ОО

8.2.1.1 Обоснование функциональных требований безопасности ОО

В таблице 8.3 представлено отображение функциональных требований безопасности ОО на цели безопасности для ОО.

Таблица 8.3 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
FAU_GEN.1				X				
FAU_GEN.2				X				
FAU_SAR.1				X				
FAU_SAR.2					X			
FAU_SAR.3				X				
FAU_SEL.1				X				
FAU_STG.1					X			
FAU_STG.3					X			
FAU_STG.4					X			
FDP_ACC.1	X							
FDP_ACF.1	X							
FIA_AFL.1 (1)			X					
FIA_ATD.1	X	X		X				
FIA_UAU.2 (1)			X					
FIA_UID.2	X	X						
FIA_USB.1	X	X		X				
FMT_MOF.1						X		
FMT_MSA.1	X					X		

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
FMT_MSA.3	X					X		
FMT_MTD.1						X		X
FMT_REV.1 (1)						X		
FMT_REV.1 (2)	X							
FMT_SMR.1	X				X	X	X	
FPT_RVM.1 (1)							X	
FPT_SEP.1 (1)							X	
FRU_RSA.2 (1)								X
FRU_RSA.2 (2)								X
FTA_TSE.1		X						

FAU_GEN.1 Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченному администратору ОО всей информации аудита впонятном для него виде. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает запрет всем пользователям доступ к чтению записей аудита, за исключением уполномоченных администраторов ОО, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение поиска данных аудита, основанного на определенных критериях в логическом отношении «И» (наименование поля данных, значение поля данных). Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, уполномоченным администратором ОО по таким атрибутам, как категория события, класс события, поле данных. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает защиту хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FAU_STG.3 Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает создание нового журнала аудита, если журнал аудита превысит установленный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает игнорирование событий, подвергающихся аудиту, и останов ОО при отсутствии свободного дискового пространства для создания журнала аудита. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FDP_ACC.1 Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает реализацию политики дискреционного доступа для субъектов, именованных объектов и всех операций между

субъектами и объектами. Рассматриваемый компонент сопоставлен с целью **O.AccessObject** и способствует ее достижению.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Выполнение требований данного компонента обеспечивает осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, определении правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **O.AccessObject** и способствует ее достижению.

FIA_AFL.1 (1) Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает блокировку регистрационной записи пользователя ОО при превышении установленного числа неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целью **O.TOEAuth** и способствует ее достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (пользователя ОО и администратора ОО) в качестве атрибутов безопасности идентификатора регистрационной записи пользователя, идентификатора учетной записи пользователя, идентификатора роли, участником которой является пользователь. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AccessTOE, O.AuditEvents, O.AdminManage** и способствует их достижению.

FIA_UAU.2 (1) Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа к ОО и объектам ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **O.TOEAuth** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации субъекта доступа к ОО и объектам ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AccessTOE** и способствует их достижению.

FIA_USB.1 Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от

имени этого субъекта доступа. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AccessTOE, O.AuditEvents** и способствует их достижению.

FMT_MOF.1 Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает модификацию и определение режимов выполнения функций, связанных с аудитом и аутентификацией субъектов доступа, только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AdminManage** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для уполномоченного администратора ОО и пользователя ОО, являющегося владельцем объекта, определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AdminManage** и способствует их достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации определенных данных ФБО только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage и O.DistrResourse** и способствует их достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО и объектами, в пределах ОДФ только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только пользователю ОО, являющемуся владельцем объекта. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FMT_SMR.1 Роли безопасности

Данный компонент включен в ЗБ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.ProtectAudit, O.AdminManage, O.ProtectResTSF** и способствует их достижению.

FPT_RVM.1 (1) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **O.ProtectResTSF** и способствует ее достижению.

FPT_SEP.1 (1) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **O.ProtectResTSF** и способствует ее достижению.

FRU_RSA.2 (1) Минимальные и максимальные квоты

Выполнение требований данного компонента обеспечивает возможность реализации минимальных и максимальных квот для объема физической памяти, который ОО может использовать в процессе функционирования. Рассматриваемый компонент сопоставлен с целью **O.DistrResourse** и способствует ее достижению.

FRU_RSA.2 (2) Минимальные и максимальные квоты

Выполнение требований данного компонента обеспечивает возможность реализации минимальных и максимальных квот для объема дискового пространства, который базы данных могут использовать одновременно. Рассматриваемый компонент сопоставлен с целью **O.DistrResourse** и способствует ее достижению.

FTA_TSE.1 Открытие сеанса с ОО

Выполнение требований данного компонента обеспечивает способность отказа ОО в открытии сеанса доступа к ОО, основываясь на идентификаторе регистрационной записи пользователя и предельном количестве одновременно открытых сеансов доступа к

ОО. Рассматриваемый компонент сопоставлен с целью **O.AccessTOE** и способствует ее достижению.

8.2.1.2 Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ЗБ соответствуют ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), и сформулированы, исходя из соответствия настоящего ЗБ профилю защиты «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005».

Выбор ОУД1 в качестве основы требований доверия в настоящем ЗБ является достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.

8.2.2 Обоснование требований безопасности для среды ИТ

В таблице 8.4 представлено отображение функциональных требований безопасности среды ИТ на цели безопасности для среды.

Таблица 8.4 – Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	OE.OSAuth	OE.ManageAuth	OE.ProtectResTS	OE.GenerateTim
FIA_AFL.1 (2)	**X**	**X**		
FIA_SOS.1	**X**	**X**		
FIA_UAU.2 (2)	**X**			
FPT_RVM.1 (2)			**X**	
FPT_SEP.1 (2)			**X**	
FPT_STM.1				**X**

FIA_AFL.1 (2) Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает блокировку регистрационной записи пользователя ОО при превышении установленного числа

неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целями **OE.OSAuth, OE.ManageAuthData** и способствует их достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает верификацию качества паролей на доступ к ОО. Рассматриваемый компонент сопоставлен с целями **OE.OSAuth, OE.ManageAuthData** и способствует их достижению.

FIA_UAU.2 (2) Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа к ОО и объектам ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **OE.OSAuth** и способствует ее достижению.

FPT_RVM.1 (2) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **OE.ProtectResTSF** и способствует ее достижению.

FPT_SEP.1 (2) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **OE.ProtectResTSF** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени. Рассматриваемый компонент сопоставлен с целью **OE.GenerateTime** и способствует ее достижению.

8.2.3 Обоснование зависимостей требований

В таблице 8.5 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены в настоящем ЗБ либо включением компонентов, определенных в части 2 ОК под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 ОК под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 8.5 является справочным и содержит компоненты, определенные в части 2 ОК в описании компонентов требований, приведенных в столбце 1 таблицы 8.5, под рубрикой «Зависимости».

Столбец 3 таблицы 8.5 показывает, какие компоненты требований были реально включены в настоящий ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 8.5. Компоненты требований в столбце 3 таблицы 8.5 либо совпадают с компонентами в столбце 2 таблицы 8.5, либо иерархичны по отношению к ним.

Таблица 8.5 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
Зависимости функциональных требований ОО		
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1 (1)	FIA_UAU.1	FIA_UAU.2 (1)
FIA_UAU.2 (1)	FIA_UID.1	FIA_UID.2
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
Зависимости функциональных требований среды ИТ		
FIA_AFL.1 (2)	FIA_UAU.1	FIA_UAU.2 (2)
FIA_UAU.2 (2)	FIA_UID.1	FIA_UID.2

Таким образом, все зависимости включенных в ЗБ функциональных требований были удовлетворены.

8.3 Обоснование краткой спецификации ОО

Обоснование краткой спецификации ОО представлено таблицей 8.6 и таблицей 8.7.

Таблица 8.6 – Отображение функциональных требований безопасности на функции безопасности

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО	Использование ресурсов ОО
Функциональные требования ОО							
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FAU_SEL.1	X						
FAU_STG.1	X						
FAU_STG.3	X						
FAU_STG.4	X						
FDP_ACC.1		X					
FDP_ACF.1		X					
FIA_AFL.1 (1)			X				

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО	Использование ресурсов ОО
FIA_ATD.1			X				
FIA_UAU.2 (1)			X				
FIA_UID.2			X				
FIA_USB.1			X				
FMT_MOF.1				X			
FMT_MSA.1				X			
FMT_MSA.3				X			
FMT_MTD.1				X			
FMT_REV.1 (1)				X			
FMT_REV.1 (2)				X			
FMT_SMR.1				X			
FPT_RVM.1 (1)					X		
FPT_SEP.1 (1)					X		
FRU_RSA.2 (1)							X
FRU_RSA.2 (2)							X
FTA_TSE.1						X	
Функциональные требования среды ИТ							
FIA_AFL.1 (2)			X				
FIA_SOS.1			X				
FIA_UAU.2 (2)			X				
FPT_RVM.1 (2)					X		

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО	Использование ресурсов ОО
FPT_SEP.1 (2)					**X**		
FPT_STM.1					**X**		

Таблица 8.7 – Отображение требований доверия на меры безопасности

	Управление конфигурацией	Предоставление руководств	Предоставление проектной документации	Тестирование
ACM_CAP.1	**X**			
ADO_IGS.1		**X**		
ADV_FSP.1			**X**	
ADV_RCR.1			**X**	
AGD_ADM.1		**X**		
AGD_USR.1		**X**		
ATE_IND.1				**X**

8.4 Обоснование требований к стойкости функций безопасности

Термин «стойкость функции» определен в части 1 ОК как характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного режима при прямой атаке на лежащие в ее основе механизмы безопасности. В части 1 ОК определено три уровня стойкости функции: базовая СФБ, средняя СФБ и высокая СФБ. В настоящем ЗБ выбран уровень стойкости функции – средняя СФБ. Средняя СФБ – это уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения. Выбор СФБ в ЗБ определялся, исходя из возможностей ОО. Выбор средней СФБ в качестве минимального уровня стойкости функций безопасности является достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.