ЗАО «АЛТЭКС-СОФТ»

Программный комплекс DEVICELOCK 6.4.1

Задание по безопасности

D_L_6.4.1.ЗБ

Версия 1.0

2010

Подп и дата	
Инв № дубл.	
Взам инв №	
Подп и дата	
Инв. № подл.	

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 5
1.1 Идентификация ЗБ 5
1.2 Аннотация ЗБ 6
1.3 Соответствие ОК 6
1.4 Соглашения 6
1.5 Организация ЗБ 7
2 ОПИСАНИЕ ОО 9
2.1 Основные функциональные возможности ОО 9
2.2 Границы ОО 13
2.2.1 Логические границы ОО 13
2.2.2 Физические границы ОО 13
3 СРЕДА БЕЗОПАСНОСТИ ОО 14
3.1 Предположения безопасности 14
3.2 Угрозы 14
3.3 ПОЛИТИКА БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ 14
3.4 Предположения и разъяснения области применения 15
3.4.1 Предположения по физической защите 15
3.4.3 Предположения связности 16
4 ЦЕЛИ БЕЗОПАСНОСТИ 17
4.1 Цели безопасности для ОО 17
4.2 Цели безопасности, относящиеся к среде 17
5 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ 19
5.1 Требования безопасности для ОО 19
5.1.1 Функциональные требования безопасности 21
5.1.2.1 Класс FAU: Аудит безопасности 21
5.1.2.2 Класс FDP: Защита данных пользователя 24
5.1.2.3 Класс FMT: Управление безопасностью 26
5.1.2.4 Класс FPT: Защита ФБО 29
5.1.2 Требования доверия к безопасности ОО 29
5.1.2.1 Управление конфигурацией (ACM) 30
5.1.2.2 Поставка и эксплуатация (ADO) 31
5.1.2.3 Разработка (ADV) 31
5.1.2.4 Руководства (AGD) 33
5.1.2.5 Тестирование (ATE) 35
5.1.2.6 Оценка уязвимостей (AVA) 37
5.2 Требования безопасности для ИТ-среды 38
5.2.1 Идентификация и аутентификация (FIA) 39
5.2.2 Защита ФБО (FPT) 40
5.3 Стойкость функции безопасности 41
6 КРАТКАЯ СПЕЦИФИКАЦИЯ ОО 42
6.1 Функции безопасности ОО 42
6.1.1 Аудит безопасности 42

6.1.2 Управление доступом *44*
6.1.3 Управление безопасностью *46*
6.1.4 Защита ФБО *47*
6.1 Меры доверия 47

7 ОБОСНОВАНИЕ 52

7.1 Взаимосвязь политик, предположений и целей безопасности 52
7.2 Обоснование целей безопасности 53
7.3 Обоснование требований безопасности 55
7.3.1 Обоснование функциональных требований безопасности ОО *55*
7.3.2 Обоснование требований безопасности среды ОО *61*
7.3.3 Обоснование требований доверия к безопасности ОО *65*
7.4 Обоснование зависимости требований 65
7.5 Обоснование краткой спецификации ОО 66

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	база данных
ЗБ	задание по безопасности
ИТ	информационная технология
НСД	несанкционированный доступ
ОК	Общие критерии
ОО	объект оценки
ОУД	оценочный уровень доверия
ПБО	политика безопасности объекта оценки
ПЗ	профиль защиты
ПО	программное обеспечение
ПФБ	политика функции безопасности
РД	руководящий документ
СУБД	система управления базами данных
СФБ	стойкость функции безопасности
УК	управление конфигурацией
ФБО	функции безопасности объекта оценки
ФТБ	функциональное требование безопасности
ACL	Access Control Lists

1 Введение

Данный документ представляет собой задание по безопасности версии 1.0, разработанное в соответствии с Общими критериями, на ИТ-продукт Программный комплекс «DeviceLock 6.4.1».

1.1 Идентификация ЗБ

Название ЗБ:	Программный комплекс «DeviceLock 6.4.1». Задание по безопасности.
Версия ЗБ:	Версия 1.0.
Обозначение ЗБ:	D_L_6.4.1.ЗБ
Идентификация ОО:	Программный комплекс «DeviceLock 6.4.1».
Уровень доверия:	ОУД2
Идентификация ОК:	Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, Гостехкомиссия России, 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.
Ключевые слова	Сменные носители информации, внешние устройства, контроль доступа, копирование информации, ОУД2.

1.2 Аннотация ЗБ

Объектом оценки (ОО) в настоящем ЗБ является встроенные функции безопасности программного комплекса «DeviceLock 6.4.1», представляющего собой средство контроля и протоколирования доступа пользователей к портам, сменным носителям и устройствам хранения данных на персональных компьютерах на аппаратной платформе x86 (32 и 64 бит), работающих под управлением операционных систем (ОС):

- Microsoft Windows XP Professional Edition SP3;
- Microsoft Windows Vista Business Edition SP2;
- Microsoft Windows Vista Ultimate Edition SP2;
- Microsoft Windows 7 Professional Edition SP2;
- Microsoft Windows Server 2003 R2 Standard Edition SP2;
- Microsoft Windows Server 2003 R2 Enterprise Edition SP2;
- Microsoft Windows Server 2008 Standard Edition SP2;
- Microsoft Windows Server 2008 Enterprise Edition SP2;
- Microsoft Windows Server 2008 R2 Standard Edition SP2;
- Microsoft Windows Server 2008 R2 Enterprise Edition SP2.

Поддерживаются 32 и 64-битные версии указанных ОС, работающих на аппаратной платформе x86.

1.3 Соответствие ОК

Объект оценки и ЗБ согласованы и соответствуют следующим спецификациям:

- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности (соответствие части 2);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности (соответствие части 3, ОУД2).

1.4 Соглашения

Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002) (далее – Общие критерии) допускает выполнение определенных в части 2 ОК операций с функциональными компонентами. Соответственно в настоящем ЗБ используются операции **«итерация» «уточнение», «выбор»** и **«назначение».**

Операция «**итерация**» используется для повторного использования одного и того же функционального компонента с целью охватить различные аспекты одного и того же требования (например, идентифицировать несколько типов функций управления безопасностью). Результат операции **«итерация»** в настоящем ЗБ обозначается порядковым номером в круглых скобках вслед за кратким именем компонента.

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 не конкретизированному параметру. Результат операции **«назначение»** в настоящем ЗБ обозначается заключением значения параметра в квадратные скобки, [назначаемое значение].

1.5 Организация ЗБ

Настоящее ЗБ разработано в соответствии с требованиями Части 1 ОК, Приложение В и содержит следующие разделы:

Раздел 1 – «Введение ЗБ» содержит описательную информацию, необходимую для идентификации ЗБ и ОО, к которому оно относится;

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 продукта;

Раздел 3 – «Среда безопасности ОО» содержит описание аспектов среды безопасности ОО. В данном разделе определяется политика безопасности организации, которой должен следовать ОО, и предположения (обязательные условия) безопасного использования ОО;

Раздел 4 – «Цели безопасности» содержит определение совокупности целей безопасности для ОО и среды функционирования ОО;

Раздел 5 – «Требования безопасности ИТ» содержит определение функциональных требований безопасности ИТ и требований доверия к безопасности ОО на основе частей 2 и 3 ОК соответственно.

Раздел 6 – «Краткая спецификация ОО» включает описание реализуемых ОО функций безопасности ИТ и мер доверия к безопасности, соответствующих специфицированным в ЗБ функциональным требованиям безопасности и требованиям доверия к безопасности ОО.

Раздел «Утверждения о соответствии ПЗ» в настоящем ЗБ отсутствует, поскольку ПЗ для продуктов аналогичных программному комплексу «DeviceLock 6.4 не разрабатывался.

Раздел 7 – «Обоснование» демонстрирует, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает идентифицированные аспекты безопасности ИТ-среды, а также что функции безопасности ИТ и меры доверия соответствуют требованиям безопасности ОО.

2 Описание ОО

Объект оценки – встроенные функции безопасности программного комплекса «DeviceLock 6.4.1», предназначеного для защиты и администрирования локальных и сетевых компьютеров, представляющий собой средство контроля и протоколирования доступа пользователей к портам, сменным носителям и устройствам хранения данных на персональных компьютерах.

2.1 Основные функциональные возможности ОО

Программный комплекс «DeviceLock 6.4.1» состоит из трех компонентов (рисунок 2.1): агента (DeviceLock Service), сервера (DeviceLock Enterprise Server и DeviceLock Content Security Server) и консоли управления (DeviceLock Management Console, DeviceLock Group Policy Manager или DeviceLock Enterprise Manager):

Агент DeviceLock Service, являясь основным компонентом программного комплекса «DeviceLock 6.4.1», устанавливается на каждый клиентский компьютер, автоматически запускается при загрузке ОС

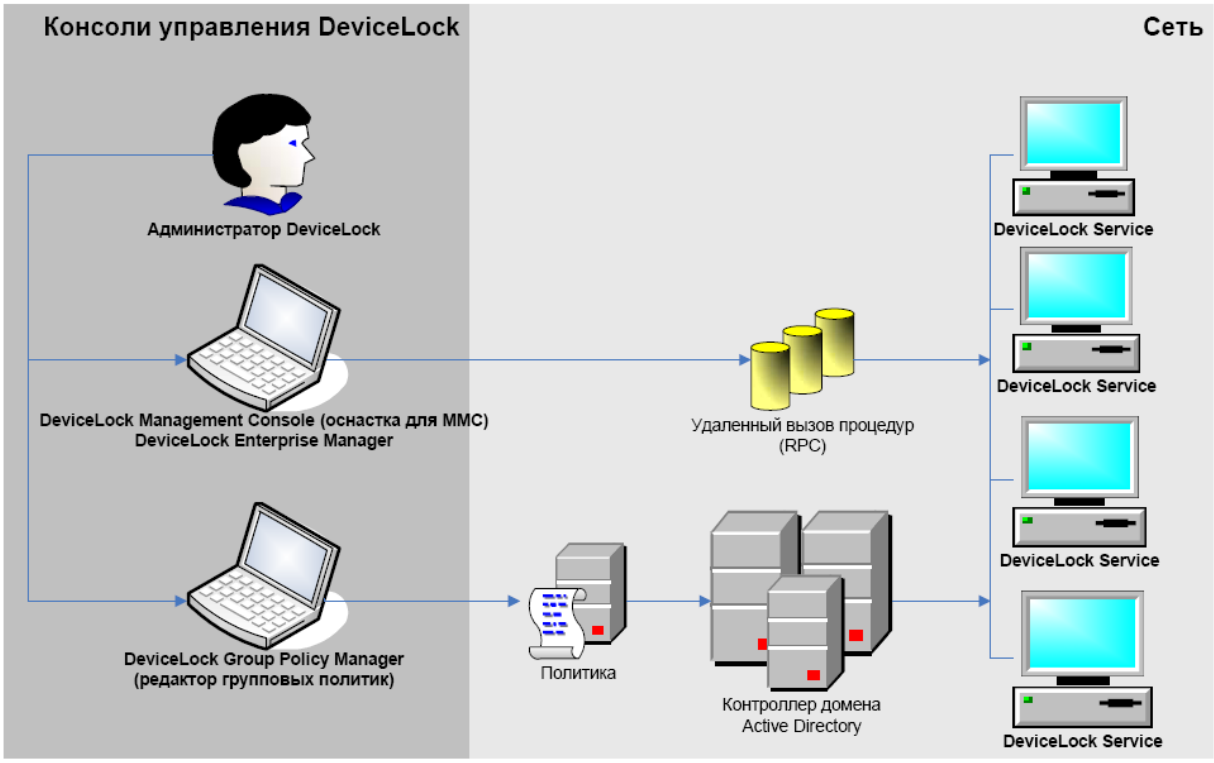

Рисунок 2.1 - Программный комплекс «DeviceLock 6.4.1»

DeviceLock Enterprise Server – компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита. DeviceLock Enterprise Server

использует MS SQL Server для хранения данных. Для обеспечения равномерной нагрузки сети и ПЭВМ допускается установка нескольких экземпляров DeviceLock Enterprise Server.

DeviceLock Content Security Server – отдельно лицензируемый компонент, включающий в себя поисковый сервер для быстрого поиска текста в файлах теневого копирования и журналах, хранящихся на DeviceLock Enterprise Server.

Консоль управления – это интерфейс контроля, который системный администратор использует для удаленного управления любой системой, на которой установлен агент (DeviceLock Service). DeviceLock поставляется с тремя различными консолями управления: DeviceLock Management Console (оснастка для MMC), DeviceLock Enterprise Manager и DeviceLock Group Policy Manager (интегрирован в редактор групповых политик Windows). DeviceLock Management Console также используется для управления DeviceLock Enterprise Server и DeviceLock Content Security Server.

ОО позволяет:

- контролировать доступ пользователей или групп к внутренним устройствам — контроллерам Wi-Fi, Bluetooth, CD- и DVD-дисководам, жестким дискам; внешним USB-носителям, портам ввода-вывода USB, IEEE 1394, COM, LPT, IrDA; локальным и сетевым принтерам.
- контролировать доступ пользователей и групп к устройствам и портам ввода-вывода в зависимости от времени суток и дня недели;
- устанавливать тип доступа «только чтение» для сменных носителей, дисководов, жестких дисков и CD/DVD-приводов;
- защищать диски и сменные носители от случайного или преднамеренного форматирования;
- задавать личный для каждого пользователя или группы список устройств, доступ к которым будет всегда разрешен. Устройства могут идентифицироваться по модели и по уникальному серийному номеру;
- идентифицировать на основе анализа записанных данных CD/DVD-диск и разрешать его использование, даже если сам CD/DVD-привод заблокирован;
- предоставлять пользователю временный доступ к устройствам по специальному буквенно-цифровому коду, переданному по телефону администратором, при отсутствии сетевого подключения агента;

- протоколировать все действия пользователей с устройствами и файлами (копирование, чтение, удаление и т.п.), с изменениями настроек агента, его времени запуска и остановки;
- сохранять для каждого пользователя или группы точную копию данных, передаваемых на внешние устройства или через различные порты (теневое копирование). Точные копии всех файлов и данных сохраняются в SQL-базе данных (БД);
- устанавливать "контентно-зависимые" правила на уровне файловых операций. Это позволяет разрешать и запрещать доступ к определенным типам файлов вне зависимости от установленных на устройство разрешений. Контентно-зависимые правила можно использовать для включения и отключения теневого копирования для заданных типов файлов. Определение типов файлов основано на сигнатурном методе и не зависит от расширения файла. Поддерживается более 3000 различных типов файлов;
- централизованно хранить журналы аудита и теневого копирования. Для централизованного сбора и хранения данных теневого копирования и журналов аудита используется SQL-сервер и компонент DeviceLock Enterprise Server. Можно установить несколько экземпляров DeviceLock Enterprise Server в сети для равномерного распределения нагрузки;
- обеспечивать необходимый уровень защиты, даже если пользователи в сети имеют административные привилегии на локальных компьютерах. Когда защита ОО включена, никто, кроме авторизованных администраторов, не может управлять агентом или обойти его защиту;
- обеспечивать посредством системы удаленного управления доступ ко всем возможным функциям агента с рабочего места администратора ОО. Инструментом администратора ОО является оснастка DeviceLock Management Console для Microsoft Management Console со стандартным интерфейсом Windows. Кроме того, для управления ОО в сетях, где не используется Active Directory, предусмотрена консоль DeviceLock Enterprise Manager с собственным интерфейсом;
- управлять агентом через групповые политики Windows в домене Active Directory посредством стандартной оснастки Group Policy, которая входит в состав серверных операционных систем начиная с Windows 2000 Server. Полная

интеграция в групповые политики Windows позволяет автоматически устанавливать ОО на новые компьютеры, подключаемые к корпоративной сети, и осуществлять настройку для новых компьютеров в автоматическом режиме;

- обеспечивать поддерживать контекстно-зависимую систему политик безопасности (в зависимости от наличия или отсутствия подключения компьютера к корпоративной сети, доступности контроллера домена, доступности DeviceLock Enterprise Server);
- выбирать компьютеры напрямую из служб каталогов LDAP;
- формировать отчеты по установленным настройкам и по устройствам (USB, IEEE 1394), которые используют пользователи на своих клиентских компьютерах.
- формировать отчеты (в т.ч. и графические) по установленным настройкам и по устройствам (USB, IEEE 1394), которые используют пользователи на своих клиентских компьютерах.
- осуществлять контроль, аудит и теневое копирование для локальных и сетевых принтеров. Контролировать отправку документов на печать по пользователям и времени. Поддерживаются все интерфейсы (USB, LPT, сеть). Включить аудит и теневое копирование для печатаемых документов.

ОО работает в среде ОС семейства Windows:

- Microsoft Windows XP Professional Edition SP3;
- Microsoft Windows Vista Business Edition SP2;
- Microsoft Windows Vista Ultimate Edition SP2;
- Microsoft Windows 7 Professional Edition SP2;
- Microsoft Windows Server 2003 R2 Standard Edition SP2;
- Microsoft Windows Server 2003 R2 Enterprise Edition SP2;
- Microsoft Windows Server 2008 Standard Edition SP2;
- Microsoft Windows Server 2008 Enterprise Edition SP2;
- Microsoft Windows Server 2008 R2 Standard Edition SP2;
- Microsoft Windows Server 2008 R2 Enterprise Edition SP2.

Поддерживаются 32 и 64-битные версии указанных ОС, работающих на аппаратной платформе x86.

2.2 Границы ОО

2.2.1 Логические границы ОО

Логические границы ОО составляют ФБО ОО:

– аудит безопасности;
– управление доступом;
– управление безопасностью;
– защита ФБО.

Подробное описание ФБО приведено в разделе 6 настоящего ЗБ.

2.2.2 Физические границы ОО

Физические границы ОО в общем варианте включают себя 3 группы ПЭВМ:

Группа 1 – ПЭВМ для обеспечения контролируемого доступа к устройствам. На ПЭВМ данной группы устанавливается компонент DeviceLock Service;

Группа 2 – для обеспечения централизованного управления контролируемого доступа к устройствам и портам управляемых ПЭВМ. Группа состоит из 1 или 2 серверных ПЭВМ , на которые устанавливаются серверные компоненты ОО: DeviceLock Enterprise Server и DeviceLock Content Security Server;

Группа 3 – рабочие места администратора ОО (1 или несколько ПЭВМ). На ПЭВМ данной группы устанавливаются консоли управления ОО: DeviceLock Management Console, DeviceLock Group Policy Manager, DeviceLock Enterprise Manager.

Допускается объединение групп ПЭВМ в 1 или 2 группы в любых сочетаниях для обеспечения частных вариантов организации контролируемого доступа к устройствам.

ПЭВМ объединяются в локальную сеть и имеют аппаратные характеристики не ниже:

– 32-разрядный (x86) или 64-разрядный (x64) процессор с частотой 1ГГц;
– 1 Гбайт оперативной памяти;
– жесткий диск объемом не менее 40 Гбайт с 15 Гбайтами свободного дискового пространства;
– привод DVD;
– сетевой адаптер.

3 Среда безопасности ОО

Формулировка среды безопасности ОО описывает аспекты безопасности среды, в которой предполагается использование ОО ожидаемым способом.

Формулировка среды безопасности ОО определяет предположения, сделанные о среде функционирования и предполагаемом способе использования продукта, угрозы, которым продукт должен противостоять, и политики безопасности организации, которым продукт должен следовать.

3.1 Предположения безопасности

Активами ОО, защищаемыми согласно ПБО, являются:

– журналы аудита;
– данные теневого копирования;
– настройки функционирования ОО;
– настройки ПБО.

3.2 Угрозы

Цели безопасности ОО определены из политики безопасности организации, представленной в следующем подразделе. Исходя из этого изложение конкретных угроз в настоящем ЗБ отсутствует.

3.3 Политика безопасности организации

Политикой безопасности организации является набор правил или процедур, предписанных организацией для защиты чувствительных данных.

P.AUDIT Реализованные в составе ОО механизмы аудита должны предоставлять Администратору возможность управления множеством событий, подвергаемых аудиту, а также предоставлять клиенту возможность получения статистической информации по установленным и действующим защищенным соединениям.

P.ADMIN Управление ОО или его компонентами должно осуществляться Администратором или пользователями, имеющими уровень знаний и подготовки достаточный для корректного использования ОО в соответствии со своими обязанностями.

P.DISTR Администратор ОО должен осуществлять первоначальную настройку значений параметров конфигурации ОО, сопровождение, поддерживать нормальный режим функционирования и осуществлять контроль работы ОО.

P.AUTHOR Доступ и работа с устройствами, контролируемыми ОО, возможны только для уполномоченных для этого пользователей.

P.NEED ОО должен ограничивать доступ к ресурсам в соответствии со служебными обязанностями пользователей.

P.ACCOUNT Пользователи несут ответственность за свои действия с использованием ОО.

P.ACCESS Полномочия на доступ к конкретному объекту доступа ОО должны основываться на механизме аутентификации пользователей ОС. Доступ пользователей к ОО и объектам ОО должен осуществляться в соответствии с назначенными в ОО правами доступа.

P.SHADOW Должна быть организована возможность теневого копирования данных пользователя передаваемых (читаемых) на (с) внешние устройства, обеспечивающая возможность их восстановления в случае фатального разрушения.

P.INSTALL Инсталляция продукта произведена в соответствии с регламентированными процедурами поставки, инсталляции и функционирования в соответствии с документацией на ОО.

P.PROTECT Данные, необходимые для разрешения временного доступа к устройствам, а также файлы настроек должны быть защищены от модификации.

3.4 Предположения и разъяснения области применения

В ходе оценки были учтены следующие предположения относительно применения ОО, сделанные в ЗБ

3.4.1 Предположения по физической защите

A.LOCATE Вычислительные ресурсы ОО должны быть сосредоточены в контролируемой зоне.

A.PROTECT Программное обеспечение ОО, критичное к осуществлению политики

безопасности, должно быть защищено от несанкционированной физической модификации.

3.4.2 Предположения о персонале

A.MANAGE Для управления ОО и безопасностью информации должны быть назначены компетентные лица.

A.NO_EVIL_ADM Системный административный персонал должен быть ответственным, управляемым и невраждебным и строго придерживается инструкций из административной документации.

A.COOP Уполномоченные пользователи должны обладать необходимыми полномочиями на доступ, по крайней мере, к некоторой части информации, управляемой ОО, и совместно работать в доверенной среде.

3.4.3 Предположения связности

A.PEER Любые системы, с которыми ОО взаимодействует, находятся под таким же управлением и функционируют по тем же правилам политики безопасности, что и ОО.

A. CONNECT Все связи с периферийными устройствами остаются в пределах контролируемой зоны. ОО предполагают условия безопасности, предусматривающие обращение к объекту оценки через санкционированные точки. Внутренние пути к точкам доступа, таким как терминалы, надежно защищены.

A.COPY_REC В организации осуществляется резервное копирование БД с периодичностью, обеспечивающей возможность их восстановления в случае фатального разрушения БД.

A.TIME Средствами ОС обеспечиваются надежные метки времени.

4 Цели безопасности

В данном разделе определяются цели безопасности для ОО и среды его функционирования. ОО является функционально завершенным, и его правильное функционирование не зависит от каких-либо других продуктов ИТ, кроме ОС и используемой ОО СУБД.

4.1 Цели безопасности для ОО

O.INSTALL ОО не должен допускать процедуры поставки, инсталляции и функционирования, отличные от описанных в документации.

O.AUTHOR ОО должен обеспечивать контролируемый доступ и работу с устройствами для уполномоченных для этого пользователей.

O.ACCESS ФБО должны управлять доступом к ресурсам, который основан на идентификаторах пользователей и групп, предоставляемых ОС. ФБО должны разрешать уполномоченным пользователям определять доступность защищаемых ресурсов.

O.MANAGE ФБО должны предоставлять все необходимые функции и возможности для поддержки уполномоченных администраторов, ответственных за управление безопасностью ОО.

O.AUDITING ФБО должны регистрировать действия пользователей, относящиеся к безопасности ОО, и предоставлять эту информацию уполномоченным администраторам.

O.ACCOUNT ФБО должны обнаруживать и записывать в журнал аудита попытки несанкционированного доступа к объектам ОО со стороны неуполномоченных на доступ к объектам пользователей**.**

O.SHADOW ФБО должны обеспечивать теневое копирование передаваемых данных, их учет и защиту от раскрытия, модификации и подмены при хранении.

O.ENFORCE ФБО должны быть спроектированы и реализованы для обеспечения осуществления политики безопасности организации в предопределенной среде.

O.*PROTECT* ФБО должны защитить ***файлы настроек*** ОО, а также данные, необходимые для обеспечения временного доступа к устройствам, ***от модификации***.

4.2 Цели безопасности, относящиеся к среде

OE.CONFIG ОС, под управлением которой функционирует ОО, должна устанавливаться, конфигурироваться и управляться согласно руководств, обеспечивая

уникальные идентификаторы пользователей, и настройки, защищающие ОО от несанкционированного доступа.

OE.IDENTITY ОС, под управлением которой функционирует ОО, должна обеспечивать надлежащие механизмы идентификации субъектов доступа к ОО.

OE.AUTHENT ОС, под управлением которой функционирует ОО, должна обеспечивать надлежащие механизмы аутентификации субъектов доступа к ОО, позволяющие защитить аутентификационную информацию и ОО от прямых или умышленных атак нарушителя с умеренным потенциалом нападения.

OE.ROLE ОС, под управлением которой функционирует ОО, должна обеспечивать поддержку роли администратора ОО.

OE.TIME ОС, под управлением которой функционирует ОО, должна обеспечивать предоставление надлежащего источника меток времени, в том числе и для ОО.

OE.ADMIN Для осуществления безопасного управления ОС и собственно ОО должны быть назначены ответственные лица с достаточным уровнем компетентности и благонадежности.

OE.RECOVER ОС, под управлением которой функционирует ОО, должна предусматривать процедуры и механизмы безопасного восстановления ОО после сбоев (отказов) программного и аппаратного обеспечения, а также других прерываний функционирования.

OE.PROTECT Все программное, аппаратное обеспечение и периферийное оборудование, взаимодействующее с ОО, должно быть доверенным, защищенным от несанкционированного физического доступа и не должно содержать угроз безопасности обрабатываемой и передаваемой информации.

OE.COPY_REC Для безопасного функционирования ОО должно быть организовано резервное копирование БД с периодичностью, обеспечивающий возможность их восстановления в случае фатального разрушения БД.

5 Требования безопасности ИТ

В данном разделе представлены функциональные требования и требования доверия к безопасности, которые должны быть удовлетворены ОО и ИТ-средой его функционирования. Данные требования представляют собой набор функциональных компонент части 2 Руководящий документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» «Функциональные требования безопасности, а также Оценочный Уровень Доверия 2 (ОУД2) требований доверия к безопасности Части 3 «Требования доверия к безопасности» того же Руководящего документа.

5.1 Требования безопасности для ОО

Данный пункт содержит функциональные требования безопасности и требования доверия к безопасности, которые должны удовлетворяться посредством ОО.

В таблице 5.1 представлен сводный перечень функциональных компонентов.

Таблица 5.1. - Сводный перечень функциональных компонентов

Функциональный класс	**Функциональное семейство**	**Функциональный компонент**
Класс FAU: Аудит безопасности	Генерация данных аудита безопасности (FAU_GEN)	FAU_GEN.1 Генерация данных аудита
		FAU_GEN.2 Ассоциация идентификатора пользователя
	Просмотр аудита безопасности (FAU_SAR)	FAU_SAR.1 Просмотр аудита
		FAU_SAR.2 Ограниченный просмотр аудита
		FAU_SAR.3 Выборочный просмотр аудита
	Выборочный аудит безопасности (FAU_SEL)	FAU_SEL.1 Избирательный аудит
	Хранение данных аудита безопасности (FAU_STG)	FAU_STG.1 Защищенное хранение журнала аудита
		FAU_STG.3 Действия в случае возможной потери данных аудита

Функциональный класс	**Функциональное семейство**	**Функциональный компонент**
Класс FDP: Защита данных пользователя	Политика управления доступом (FDP_ACC)	FDP_ACC.1 Ограниченное управление доступом
	Функции управления доступом (FDP_ACF)	FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности
Класс FMT: Управление безопасностью	Управление атрибутами безопасности (FMT_MSA)	FMT_MSA.1 (1) Управление атрибутами безопасности
		FMT_MSA.1 (2) Управление атрибутами безопасности
		FMT_MSA.1 (3) Управление атрибутами безопасности
		FMT_MSA.2 Безопасные значения атрибутов безопасности
		FMT_MSA.3 Инициализация статических атрибутов
	Управление данными ФБО (FMT_MTD)	FMT_MTD.1 (1) Управление данными ФБО
		FMT_MTD.1 (2) Управление данными ФБО
	Роли управления безопасностью (FMT_SMR)	FMT_SMR.1 Роли безопасности
Класс FPT: Защита ФБО	Посредничество при обращениях (FPT_RVM)	FPT_RVM.1 Невозможность обхода ПБО

Функциональный класс	Функциональное семейство	Функциональный компонент
	Передача данных комплекса средств безопасности в пределах объекта оценки (FPT_ITT)	FPT_ITT.1 Базовая защита внутренней передачи данных ФБО

5.1.1 Функциональные требования безопасности

5.1.2.1 Класс FAU: Аудит безопасности

FAU_GEN.1 (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) [попытка доступа к запрещенным устройствам (тип устройства, тип действия);

доступ к разрешенным устройствам (тип устройства, тип действия);

старт и останов агента;

все административные действия, совершаемые уполномоченными администраторами;

действия, совершаемые по настройке параметров конкретного агента.]

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 (успех или неудача) события;

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ЗБ.

Зависимости:

FPT_STM.1 Надежные метки времени.

FAU_GEN.1 (2) Генерация данных аудита

FAU_GEN.1.1 ФБО генерируют записи аудита следующих журналах системы:

[

- журнал аудита;
- журнал теневого копирования;
- журнал теневого удаления;
- внутренний журнал сервера;
- журнал мониторинга.

]

FAU_GEN.1.2 Записи аудита имеют следующую структуру:

[

– дата и время события;

– идентификатор объекта;

– идентификатор пользователя;

– идентификатор узла сети;

– тип события.

– тип устройства;

– тип действия пользователя.

– идентификатор процесса приложения, связанного с событием.

]

Зависимости:

FPT_STM.1 Надежные метки времени.

FAU_GEN.2 Ассоциация идентификатора пользователя

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

Зависимости:

FAU_GEN.1 Генерация данных аудита.

FIA_UID.1 Выбор момента идентификации.

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченным администраторам] возможность читать [всю информацию] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем пользователю 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 пользователей, 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:

[

а) текстовой строке поиска с поддержкой шаблонов;

б) диапазона времени события;

в) выборке из множества журналов для осуществления поиска:

- *журнал аудита;*
- *журнал теневого копирования;*
- *журнал теневого удаления;*
- *внутренний журнал сервера;*
- *журнал мониторинга.*

]

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 их исключению из этой совокупности по следующим атрибутам:

а) – *идентификатор объекта;*

– *идентификатор пользователя;*

– *идентификатор узла сети;*

– *тип события.*

б) [

– дата и время, когда событие было получено;

– тип устройства;

– тип действия пользователя;

– идентификатор процесса приложения, связанного с событием.

]

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 [формирование предупреждения администратору ОО], если журнал аудита превышает [определенный администратором ОО размер].

Зависимости:

FAU_STG.1 Защищенное хранение журнала аудита.

5.1.2.2 Класс FDP: Защита данных пользователя

FDP_ACC.1 Ограниченное управление доступом

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

[

а) субъектов – пользователей;

б) объектов – устройств доступа: контроллерам Wi-Fi, Bluetooth, CD- и DVD-дисководам, жестким дискам; внешним USB-носителям, портам ввода-вывода USB, IEEE 1394, COM, LPT, IrDA, локальным и сетевым принтерам;

в) операций над объектами применительно к субъектам доступа:

- чтение данных с устройства;
- запись данных на устройство;
- форматирование и другие операции с прямым доступом у устройству;
- извлечение (для съемныйх устройств);
- удаленное выполенние кода на стороне устройства;
- печать – для устройств досупа «принтер».

]

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 управления доступом] к объектам, основываясь на

[

а) ассоциированных с субъектом атрибутах управления доступом (идентификаторе пользователя, принадлежности к группе, привилегиях);

б) ассоциированных с объектом атрибутах управления доступом (владельце объекта, списке управления доступом (ACL)).

].

Примечание: Список ACL для объекта может отсутствовать, быть пустым, содержать одну или более записей, определяющей:

- доступность объекта (разрешение или запрет);
- идентификатор пользователя или группы;
- права 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 выполняется, по меньшей мере, одно из следующих условий:

а) если среди записей, содержащихся в ACL, доступ пользователю явно разрешается одной записью и не запрещен записью ей предшествующей;

б) если среди записей, содержащихся в ACL, доступ группе, членом которой является субъект, разрешается одной записью и не запрещен записью ей предшествующей;

в) список ACL отсутствует;

г) субъект является владельцем объекта и может создавать объект, а также просматривать или модифицировать его список ACL

].

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

[

а) при запросе доступа уполномоченного администратора к объекту для смены владельца, ему должен быть предоставлен доступ вне зависимости от правил, перечисленных в FDP_ACF.1.2;

б) при запросе доступа уполномоченного администратора к параметрам аудита ОО для их смены или модификации, ему должен быть предоставлен доступ вне зависимости от правил, перечисленных в FDP_ACF.1.2;

].

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

[

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

а) если среди записей, содержащихся в ACL, доступ пользователю явно запрещается одной записью и не разрешен записью ей предшествующей;

б) если среди записей, содержащихся в ACL, доступ группе, членом которой является субъект, запрещается одной записью и не разрешен записью ей предшествующей

].

Зависимости:

FDP_ACC.1 Ограниченное управление доступом,

FMT_MSA.3 Инициализация статических атрибутов.

5.1.2.3 Класс FMT: Управление безопасностью

FMT_MSA.1 (1) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом], **предоставляющую** возможность *модифицировать* атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [уполномоченному администратору ОО].

Зависимости:

[FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками]

FMT_SMR.1 Роли безопасности

FMT_MSA.1 (2) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны устанавливать [групповые политики управления доступом], **предоставляющие** возможность *<u>устанавливать</u>* [атрибуты управления доступом, ассоциированные с именованным объектом].

Зависимости:

[FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками]

FMT_SMR.1 Роли безопасности

FMT_MSA.1 (3) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны устанавливать [профили доступа], **предоставляющие** возможность *<u>устанавливать</u>* [атрибуты управления доступом для различных режимов работы:

а) Regular Profile (общий профиль). Настройки применяются на клиентских компьютерах, находящихся в сети;

б) Offline Profile (автономный профиль). Эти настройки применяются на клиентских компьютерах, работающих автономно.

]

[FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками]

FMT_SMR.1 Роли безопасности

FMT_MSA.1 (4) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны устанавливать [контекстно-зависимые правила], **предоставляющие** возможность *<u>[разрешать, запрещать]</u>* доступ к файлам определенных типов.

Зависимости:

[FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками]

FMT_SMR.1 Роли безопасности

FMT_MSA.2 Безопасные значения атрибутов безопасности

FMT_MSA.2.1 ФБО должны обеспечить присвоение атрибутам безопасности только безопасных значений

Зависимости:

ADV_SPM.1 Неформальная модель политики безопасности ОО

[FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
FMT_MSA.1Управление атрибутами безопасности
FMT_SMR.1 Роли безопасности.

FMT_MSA.3 Инициализация статических атрибутов

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

FMT_MSA.3.2 ФБО должны осуществлять [администратору ОО определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

Зависимости:

FMT_MSA.1 Управление атрибутами безопасности,

FMT_SMR.1 Роли безопасности.

FMT_MTD.1 (1) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность [*выполнения операций, указанных во втором столбце таблицы 5.2*] над данными, [указанными в третьем столбце таблицы 5.2], только [уполномоченному администратору ОО].

Зависимости:

FMT_SMR.1 Роли безопасности.

Таблица 5.2 – Управляемые данные ФБО

Компонент	Операция	Данные ФБО
FAU_GEN.1	удаление, очистка, создание	журнал аудита, файлы теневого копирования
FAU_STG.3	установление, модификация	размер журнала аудита
FPT_STM.1	модификация	представление времени

FMT_MTD.1 (2) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [собственных аутентификационных данных] только [уполномоченному пользователю ОО].

Зависимости:

FMT_SMR.1 Роли безопасности.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[

а) администратора ОО;

б) пользователя ОО

].

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

Зависимости:

FIA_UID.1 Выбор момента идентификации.

5.1.2.4 Класс FPT: Защита ФБО

FPT_RVM.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_ITT.1 Базовая защита внутренней передачи данных ФБО

FPT_ITT.1.1 ФБО должны защитить свои данные от *модификации* при их передаче между разделенными частями ОО.

Зависимости: отсутствуют.

5.1.2 Требования доверия к безопасности ОО

Целевым оценочным уровнем доверия для данного продукта является ОУД2. Никаких усилений для требований доверия не определено. Требования доверия к безопасности ОО взяты из части 3 ОК (см. таблицу 5.2).

Таблица 5.2 – Требования доверия к безопасности ОО

Класс доверия	Идентификатор компонента доверия	Название компонента доверия
Управление конфигурацией	ACM_CAP.2	Элементы конфигурации

Класс доверия	Идентификатор компонента доверия	Название компонента доверия
Поставка и эксплуатация	ADO_DEL.1	Процедуры поставки
	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_HLD.1	Описательный проект верхнего уровня
	ADV_RCR.1	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_COV.1	Свидетельство покрытия
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО
	AVA_VLA.1	Анализ уязвимостей разработчиком

5.1.2.1 Управление конфигурацией (ACM)

ACM_CAP.2 Элементы конфигурации

Элементы действий разработчика

ACM_CAP.2.1D Разработчик должен предоставить маркировку для ОО.

ACM_CAP.2.2D Разработчик должен использовать систему УК.

ACM_CAP.2.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_CAP.2.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.2.2C ОО должен быть помечен маркировкой.

ACM_CAP.2.3C Документация УК должна включать в себя список конфигурации.

ACM_CAP.2.4C Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

ACM_CAP.2.5C Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

ACM_CAP.2.6C Система УК должна уникально идентифицировать все элементы конфигурации.

Элементы действий оценщика

ACM_CAP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.2 Поставка и эксплуатация (ADO)

ADO_DEL.1 Процедуры поставки

Элементы действий разработчика

ADO_DEL.1.1D Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.1.2.D Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ADO_DEL.1.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.

Элементы действий оценщика

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

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_HLD.1 Описательный проект верхнего уровня

Элементы действий разработчика

ADV_HLD.1.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.1.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.1.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.1.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.1.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.1.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.1.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.1.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

Элементы действий оценщика

ADV_HLD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.2.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня – 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_COV.1 Свидетельство покрытия

Элементы действий разработчика

ATE_COV.1.1D Разработчик должен представить свидетельство покрытия тестами.

Элементы содержания и представления свидетельств

ATE_COV.1.1C Свидетельство покрытия тестами должно показать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

Элементы действий оценщика

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

ATE_FUN.1 Функциональное тестирование

Элементы действий разработчика

ATE_FUN.1.1D Разработчик должен протестировать ФБО и задокументировать результаты.

ATE_FUN.1.2D Разработчик должен представить тестовую документацию.

Элементы содержания и представления свидетельств

ATE_FUN.1.1C Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

ATE_FUN.1.2C Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.

ATE_FUN.1.3C Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.

ATE_FUN.1.4C Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

ATE_FUN.1.5C Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

Элементы действий оценщика

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

ATE_IND.2 Выборочное независимое тестирование

Элементы действий разработчика

ATE_IND.2.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.2.1C ОО должен быть пригоден для тестирования.

ATE_IND.2.2C Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.

Элементы действий оценщика

ATE_IND.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.2.2E Оценщик должен протестировать подмножество ФБО, как необходимо, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.2.3E Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

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 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 ЗБ.

Элементы действий оценщика

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

AVA_SOF.1.2E Оценщик должен подтвердить, что утверждения относительно стойкости корректны.

AVA_VLA.1 Анализ уязвимостей разработчиком

Элементы действий разработчика

AVA_VLA.1.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску явных путей, которыми пользователь может нарушить ПБО.

AVA_VLA.1.2D Разработчик должен задокументировать местоположение явных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.1.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

Элементы действий оценщика

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

AVA_VLA.1.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета явных уязвимостей.

5.2 Требования безопасности для ИТ-среды

Функцией безопасности, реализуемой ИТ-средой ОС в интересах обеспечения безопасности ОО, является «Идентификация и аутентификация». Данная функция реализуется механизмом паролей, относящимся к вероятностному и перестановочному типу, для которого возможен анализ стойкости.

Других механизмов, реализуемых ИТ-средой в интересах обеспечения безопасности ОО, и относящихся к вероятностному и перестановочному типу, нет, поэтому заявлений об их стойкости в настоящем ЗБ не делается.

Таблица 5.3 – Компоненты требований функции безопасности ИТ-среды ОО

Идентификатор компонента требований	Название компонента требований
FIA_AFL.1	Обработка отказов аутентификации
FIA_SOS.1	Верификация секретов
FIA_UID.2	Идентификация до любых действий пользователя
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_ATD.1	Определение атрибутов пользователя
FPT_RVM.1	Невозможность обхода ПБО

Идентификатор компонента требований	Название компонента требований
FPT_FLS.1	Доступность передаваемых данных
FPT_STM.1	Надежные метки времени

5.2.1 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 **Функции безопасности ИТ-среды** 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 ИТ-среды** должны:

[

а) сделать невозможным доступ субъекта доступа к ОО, блокировав его регистрационную запись на 30 минут;

б) осуществить сброс счетчика неуспешных попыток аутентификации и разблокировать регистрационную запись субъекта по истечении 30 минут

].

Зависимости:

FIA_UAU.2 Аутентификация до любых действий пользователя.

FIA_SOS.1 Верификация секретов

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

[

а) минимальная длина – определяется настройками групповых и локальных политик безопасности для компьютера и сети, устанавливаемыми для пользователей ОС;

б) политика использования паролей ОО должна наследоваться от политики локальных и групповых политик использования паролей для пользователей ОС.

].

Зависимости: отсутствуют.

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 **Функции безопасности ИТ-среды** должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 **Функции безопасности ИТ-среды** должны требовать, чтобы каждый **субъект доступа к 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_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 **Функции безопасности ИТ-среды** должны поддерживать для каждого пользователя следующий список атрибутов безопасности: [идентификатор пользователя и идентификатор группы].

Зависимости: отсутствуют.

5.2.2 Защита ФБО (FPT)

FPT_FLS.1 Доступность передаваемых данных ФБО

FPT_FLS.1.1 **Функции безопасности ИТ-среды** должны сохранять безопасное состояние, когда происходят следующие типы сбоев:

[

- аппаратного обеспечения;
- прикладного ПО;
- ОС;
- системы электропитания.

].

Зависимости: отсутствуют.

FPT_RVM.1 Невозможность обхода ПБО

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

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 **Функции безопасности ИТ-среды** должны быть способны предоставить надежные метки времени для собственного использования **и функционирования ОО**.

Зависимости: отсутствуют.

5.3 Стойкость функции безопасности

Для ОО не определены какие-либо ФТБ, предъявляемые к ФБО, в основе которых лежат перестановочные или вероятностные механизмы, поэтому утверждение о стойкости функций безопасности в ЗБ отсутствует.

6 Краткая спецификация ОО

6.1 Функции безопасности ОО

В данном разделе представлено описание функций безопасности ОО и их сопоставление с функциональными требованиями безопасности. ОО реализует следующие функции безопасности:

- аудит безопасности;
- управление доступом;
- управление безопасностью;
- защита ФБО.

6.1.1 Аудит безопасности

АУ.1 ОО обеспечивает возможность генерации и регистрации сообщений о событиях, связанных с использованием устройств на локальном компьютере отдельными пользователями в журналах аудита. При заполнении журнала аудита событий администратору ОО выдается предупреждающее сообщение.

АУ.2 Для каждого сообщения о событии ОО регистрируется следующая информация:

– дата и время события;
– идентификатор объекта;
– идентификатор пользователя;
– идентификатор узла сети;
– тип события.
– тип устройства;
– тип действия пользователя.
– идентификатор процесса приложения, связанного с событием.

Информация о дате и времени события берется ОО из ОС всякий раз, когда генерируется новое сообщение о событии. Идентификатор пользователя берется из ACL объекта. Для хранения записей аудита ОО использует стандартный журнал Windows, что позволяет просматривать их как с помощью стандартной программы просмотра событий, так и встроенного средства.

АУ.3 ОО обеспечивает защиту от несанкционированных попыток модификации или удаления записей аудита. Данная возможность реализуется, благодаря наличию полномочий на доступ к журналам аудита только у администраторов ОО.

АУ.4 ОО обеспечивает просмотр данных аудита в виде удобном пользователю для интерпретации информации.

АУ.5 ОО обеспечивает индексирование, полнотекстовый поиск по содержимому файлов теневого копирования и журналам DeviceLock Enterprise Server (реализуется с использованием компонента DeviceLock Content Security Server).

Сопоставление с ФТБ

Функции безопасности «Аудит безопасности» удовлетворяют следующим функциональным требованиям безопасности:

FAU_GEN.1 (1) - ОО обеспечивает генерацию записей аудита для событий:

– запуск и завершение выполнения функций аудита;
– попытка доступа к запрещенным устройствам (тип устройства, тип действия);
– доступ к разрешенным устройствам (тип устройства, тип действия);
– старт и останов агента;
– все административные действия, совершаемые уполномоченными администраторами;
– действия, совершаемые по настройке параметров конкретного агента.

FAU_GEN.1 (2) – ОО обеспечивает запись в журналы программы событий ФБО АУ.2.

FAU_GEN.2 - ФБО обеспечивают ассоциирование каждого события, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

FAU_SAR.1 - инструментальные средства просмотра событий предоставляют уполномоченному администратору ОО возможность просмотра данных аудита в удобочитаемом формате.

FAU_SAR.3 – ФБО обеспечивают возможность поиска данных аудита по следующей информации:

– текстовой строке поиска с поддержкой шаблонов;
– диапазону времени события;

– выборке из множества журналов для осуществления поиска.

FAU_SEL.1 - ФБО предоставляют возможность включать события, потенциально подвергаемые аудиту, в совокупность событий, подвергающихся аудиту.

FAU_STG.1 - ФБО защищают хранимые записи аудита от несанкционированного изменения и предотвращают их модификацию.

FAU_STG.3 - ОО может быть настроен на генерацию события аудита (предупреждение о превышении размера) в случае превышения данными аудита установленного для журнала безопасности размера.

6.1.2 Управление доступом

УД.1 ФБО обеспечивают возможность доступа процесса, запущенного от имени пользователя, к объекту только в том случае, если для ассоциированных с пользователем идентификаторов (пользователя или группы) в списке управления доступом ACL определены права доступа для данного объекта. Идентификаторы пользователя и группы берутся ОО из ОС. Проверка прав доступа, выполняемая ОО, заключается в подтверждении наличия идентификатора пользователя или группы, а также типа доступа в списке управления доступом ACL конкретного объекта.

УД.2 ФБО обеспечивают возможность модификации списков ACL только уполномоченными администраторами ОО. Администраторами является все пользователи, входящие в состав группы «Администраторы», поддерживаемой ОС. Идентификация данных субъектов доступа реализуется средствами ОС.

УД.3 При создании нового объекта, ФБО обеспечивают применение устанавливаемого по умолчанию списка управления доступом ACL, предусматривающего возможность доступа к объекту только пользователя-владельца объекта и администратора ОО. Данное поведение ФБО обеспечивается путем добавления идентификаторов пользователя-владельца объекта и администратора, а также идентификаторов групп, которым принадлежит пользователь-владелец объекта, в устанавливаемый для объекта список управления доступом ACL. После создания объекта администратор может изменять список ACL, предоставляя или отзывая права доступа, с использованием интерфейса консоли ОО.

УД.4 ОО позволяет устанавливать «контентно-зависимые» правила на уровне файловых операций. Это позволяет разрешать и запрещать доступ к определенным типам файлов вне зависимости от установленных на устройство разрешений. Контентно-зависимые правила можно использовать для включения и отключения теневого копирования для заданных типов файлов. Определение типов файлов основано на сигнатурном методе и не зависит от расширения файла. Поддерживается более 3000 различных типов файлов;

УД.5 ФБО обеспечивают контекстно-зависимую систему политик безопасности (в зависимости от наличия или отсутствия подключения компьютера к корпоративной сети, доступности контроллера домена и т.д.).

Сопоставление с ФТБ

Функции безопасности «Управление доступом» удовлетворяют следующим функциональным требованиям безопасности:

FAU_SAR.1 - инструментальные средства просмотра событий предоставляют уполномоченному администратору ОО возможность просмотра данных аудита в удобочитаемом формате.

FAU_SAR.2 - ФБО предоставляют доступ к чтению записей аудита только уполномоченным администраторам ОО;

FDP_ACC.1 – ФБО обеспечивают политику управления доступом для субъектов (пользователей) и объектов доступа (контроллеров Wi-Fi, Bluetooth, CD- и DVD-дисководов, жестких дисков, внешним USB-носителей, портов ввода-вывода USB, IEEE 1394, COM, LPT, IrDA, локальных и сетевых принтеров) и операций между ними.

FDP_ACF.1 - ФБО осуществляют политику управления доступом к объектам, основываясь на:

- ассоциированных с субъектом атрибутах управления доступом (идентификаторе пользователя, принадлежности к группе, привилегиях);
- ассоциированных с объектом атрибутах управления доступом (владельце объекта, списке управления доступом (ACL)).

FMT_MSA.1 (1) - ФБО осуществляют политику управления доступом, предоставляющую возможность модифицировать атрибуты безопасности, только уполномоченному администратору ОО.

FMT_MSA.1 (2) - ФБО устанавливают групповые политики управления доступом, предоставляющие возможность устанавливать атрибуты управления доступом, ассоциированные с именованным объектом.

FMT_MSA.1 (3) - ФБО устанавливают профили доступа, предоставляющие возможность устанавливать атрибуты управления доступом для режимов работы Regular Profile (общий профиль) и Offline Profile (автономный профиль).

FMT_MSA.1 (4) - ФБО должны устанавливать контекстно-зависимые правила, предоставляющие возможность разрешать/запрещать доступ к файлам определенных типов.

FMT_MSA.2 - ФБО обеспечивают присвоение атрибутам безопасности только безопасных значений.

FMT_MSA.3 - ФБО осуществляют политику управления доступом, предусматривающую ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики управления доступом и позволяют администратору ОО определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

6.1.3 Управление безопасностью

УБ.1 ФБО обеспечивают возможности модификации атрибутов безопасности субъектов и объектов доступа только администраторам ОО а для именованных объектов ОО также и их владельцам.

УБ.2 ФБО обеспечивают возможности устанавливать ограничительные значения атрибутов безопасности по умолчанию при создании объектов и определять альтернативные начальные значения для отмены значений по умолчанию владельцам объектов.

УБ.3 ФБО обеспечивают возможности устанавливать и поддерживать роли администратора ОО и пользователя ОО. Субъект в роли администратора ОО может выполнять удаление, очистку, создание журналов аудита и файлов теневого копирования, устанавливать и модифицировать параметры журналов аудита и меток времени.

УБ.4 ФБО обеспечивают невозможность реализации каких-либо операций субъектов над объектами ОО до успешного выполнения функций, реализующих ПБО, в пределах ОДФ.

Сопоставление с ФТБ

Функции безопасности «Управление безопасностью» удовлетворяют следующим функциональным требованиям безопасности:

FMT_MTD.1(1) - ФБО предоставляют возможность выполнения операций над данными, согласно таблицы 5.2 , только уполномоченному администратору ОО.

FMT_MTD.1(2) - ФБО предоставляют возможность модификации собственных аутентификационных данных.

FPT_RVM.1 - ФБО обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

FMT_SMR.1 – ФБО поддерживает роли администратора и пользователя ОО и ассоциирует субъекты доступа с этими ролями.

6.1.4 Защита ФБО

ЗФ.1 ФБО должны защитить файлы настроек ОО, а также данные, необходимые для обеспечения временного доступа к устройствам, от модификации.

Сопоставление с ФТБ

Функции безопасности «Защита ФБО» удовлетворяют следующим функциональным требованиям безопасности:

FPT_ITT.1 ФБО обеспечивают защиту своих данных от модификации при их передаче между разделенными частями ОО.

6.2 Меры доверия

Для удовлетворения требований доверия к безопасности согласно ОУД2 применены следующие меры доверия к безопасности ОО:

- управление конфигурацией;
- поставка и эксплуатация;
- разработка;
- руководства;
- тестирование;
- оценка уязвимостей.

В таблице 6.1 представлено описание Требований доверия к безопасности ОО

Таблица 6.1 – Требования доверия к безопасности ОО.

Требование доверия	**Описание**
ACM_CAP.2	Разработчик предоставляет документацию УК, включающую в себя список конфигурации с описанием элементов конфигурации, входящих в ОО, и описание метода, используемого для уникальной идентификации элементов конфигурации. Документация УК подтверждает, что разработчик использует систему УК, уникально идентифицирующую все элементы конфигурации. Доказательство того, что ОО маркирован должным образом, обеспечивается в процессе проведения тестирования.
ADO_DEL.1	Разработчик предоставляет свидетельство по процедурам поставки, включающее описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.
ADO_IGS.1	Разработчик предоставляет свидетельство по процедурам безопасной установки, генерации и запуска, содержащее описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.
ADV_FSP.1	Разработчик предоставляет функциональную спецификацию, содержащую неформальное описание ФБО и их внешних интерфейсов, а также описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках. Функциональная спецификация является внутренне непротиворечивой и полностью представляет ФБО.
ADV_HLD.1	Разработчик предоставляет проект верхнего уровня, содержащий неформальное и внутренне непротиворечивое описание структуры ФБО в терминах подсистем с указанием функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО, а также идентифицирующий все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для

Требование доверия	Описание
	реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами и идентифицирующий все интерфейсы для подсистем ФБО, с указанием, какие из интерфейсов подсистем ФБО являются видимыми извне.
ADV_RCR.1	Разработчик представляет свидетельство анализа соответствия между всеми смежными парами имеющихся представлений ФБО, демонстрирующее, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.
AGD_ADM.1	Разработчик предоставляет согласованное со всей другой документацией, представленной для оценки, руководство администратора, которое содержит: – описание функций администрирования и интерфейсов, доступных администратору ОО; – описание безопасных способов управления ОО; – описание предупреждений относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации; – описание всех предположений о поведении субъектов доступа, которые связаны с безопасной эксплуатацией ОО; – описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения; – описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО; – описание всех требований безопасности к среде ИТ, которые относятся к администратору.
AGD_USR.1	Разработчик не предоставляет руководство пользователя ввиду

Требование доверия	Описание
	отсутствия у пользователей специфических функций, связанных с ОО.
ATE_COV.1	Разработчик предоставляет свидетельство покрытия тестами самостоятельным документом или разделом в тестовой документации. Свидетельство покрытия тестами показывает соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.
ATE_FUN.1	Разработчик провел тестирование ФБО, задокументировал результаты и представляет тестовую документацию, которая состоит из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования. Планы тестирования идентифицируют проверяемые функции безопасности и содержат изложение целей тестирования. Описания процедур тестирования идентифицируют тесты, которые необходимо выполнить, и включают в себя сценарии для тестирования каждой функции безопасности. Эти сценарии учитывают любое влияние последовательности выполнения тестов на результаты других тестов. Ожидаемые результаты тестирования показывают прогнозируемые выходные данные успешного выполнения тестов. Результаты выполнения тестов разработчиком демонстрируют, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.
ATE_IND.2	Разработчик предоставляет ОО, пригодный для тестирования, а также набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.
AVA_SOF.1	Для ОО не определены какие-либо ФТБ, предъявляемые к ФБО, в основе которых лежат перестановочные или вероятностные механизмы, поэтому утверждение о стойкости функций безопасности в ЗБ отсутствует.
AVA_VLA.1	Разработчик предоставляет свидетельство анализа уязвимостей, в котором задокументирован выполненный анализ поставляемых материалов ОО по поиску явных путей, которыми пользователь может нарушить ПБО, а также задокументировано местоположение явных

Требование доверия	Описание
	уязвимостей. Документация показывает для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

7 Обоснование

В данном разделе дано обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ЗБ. В разделе «Обоснование».

7.1 Взаимосвязь политик, предположений и целей безопасности

В таблице 7.1 представлена взаимосвязь политик, предположений и целей безопасности.

Таблица 7.1 – Взаимосвязь политик, предположений и целей безопасности

	O.INSTALL	O.ACCOUNT	O.AUTHOR	O.ACCESS	O.MANAGE	O.AUDITING	O.SHADOW	O.ENFORCE	O.PROTECT	OE.CONFIG	OE.IDENT	OE..AUTHENT	OE.ROLE	OE.TIME	OE.ADMIN	OE.RECOVER	OE.PROTECT	OE.COPY_REC
P.AUDIT		X			X	X												
P.ADMIN															X			
P.DISTR	X				X	X							X					
P.AUTHOR			X								X	X						
P.ACCOUNT		X				X												
P.ACCESS				X							X	X						
P.NEED				X														
P. SHADOW							X									X		X
P.INSTALL	X									X								
P.PROTECT								X										
A.LOCATE								X									X	
A.PROTECT																	X	
A.MANAGE															X			
A.NO_EVIL_ADM															X			
A.COOP															X			
A.PEER										X							X	
A.CONNECT																	X	
A.COPY_REC																		X
A.TIME														X				

7.2 Обоснование целей безопасности

O.INSTALL

Достижение этой цели безопасности необходимо в связи с реализацией политик безопасности организации **P.DISTR, P.INSTALL**, так как обеспечивает корректную поставку, инсталляцию, управление в соответствии с руководствами.

O.AUTHOR

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.AUTHOR**, так как обеспечивает доступ к ОО и его ресурсам только уполномоченным пользователям.

O.ACCESS

Достижение этой цели безопасности необходимо в связи с реализацией политик безопасности организации **P.ACCESS** и **P.NEED**, так как обеспечивает доступ к ресурсам, который основан на идентификаторах пользователей и групп, предоставляемых ОС.

O.MANAGE

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.DISTR**, так как обеспечивает возможность реализации функций и средств поддержки действий уполномоченных администраторов, ответственных за управление безопасностью ОО.

O.AUDITING

Достижение этой цели безопасности необходимо в связи с реализацией политик безопасности организации **P.DISTR** и **P.ACCOUNT**, так как обеспечивает регистрацию действий пользователей, относящиеся к безопасности ОО, и предоставление эту информацию уполномоченным администраторам.

O.ACCOUNT

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.ACCOUNT**, так как обеспечивает обнаружение и запись в журнал аудита попыток несанкционированного доступа к объектам ОО со стороны неуполномоченных на доступ к объектам пользователей**.**

O.SHADOW

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.SHADOW**, так как обеспечивает теневое копирование

передаваемых данных, их учет и защиту от раскрытия, модификации и подмены при хранении.

O.ENFORCE

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.LOCATE**, так как обеспечивает реализацию политики безопасности организации в предопределенной среде.

OE.CONFIG

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.INSTALL** и предположения безопасности **A.PEER**, так как обеспечивает установку, конфигурирование и управление согласно руководств ОС, в которой работает ОО, с уникальными идентификаторами пользователей, и настройками, защищающими ОО от несанкционированного доступа.

OE.IDENT

Достижение этой цели безопасности необходимо в связи с реализацией политик безопасности организации **P.AUTHOR** и **P.ACCESS**, так как обеспечивает поддержку ОС надлежащих механизмов идентификации субъектов доступа к ОО.

OE.AUTHENT

Достижение этой цели безопасности необходимо в связи с реализацией политик безопасности организации **P.AUTHOR** и **P.ACCESS**, так как обеспечивает поддержку ОС надлежащие механизмов аутентификации субъектов доступа к ОО, позволяющих защитить аутентификационную информацию и ОО от прямых или умышленных атак нарушителя с умеренным потенциалом нападения.

OE.ROLE

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **P.DISTR**, так как обеспечивает надлежащее ассоциирование пользователей ОС с ролями и поддержку роли администратора ОО.

OE.TIME

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.TIME**, так как обеспечивает предоставление ОС надлежащего источника меток времени, в том числе и для обеспечения контролируемого доступа к устройствам по времени.

OE.ADMIN

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.ADMIN** и предположений безопасности **A.MANAGE** и **A.COOP**, так как обеспечивает назначение ответственных лица с достаточным уровнем компетентности и благонадежности.

O.PROTECT

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.PROTECT**, так как обеспечивает защиту файлы настроек **OO, а также** данные, необходимые для обеспечения временного доступа к устройствам, от модификации**.**

OE.RECOVER

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.SHADOW**, так как обеспечивает процедуры и механизмы безопасного восстановления ОО после сбоев (отказов) программного и аппаратного обеспечения, а также других прерываний функционирования.

OE.PROTECT

Достижение этой цели безопасности необходимо в связи с реализацией предположений безопасности **A.LOCATE, A.PROTECT**, **A.PEER, A.CONNECT,** так как обеспечивает обеспечение того, что аппаратное обеспечение и периферийное оборудование, взаимодействующее с ОО, должно быть доверенным, защищенным от несанкционированного физического доступа и не должно содержать угроз безопасности обрабатываемой и передаваемой информации.

OE.COPY_REC

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.COPY_REC**, так как обеспечивает организацию резервного копирования БД с периодичностью, обеспечивающий возможность их восстановления в случае фатального разрушения БД.

7.3 Обоснование требований безопасности

7.3.1 Обоснование функциональных требований безопасности ОО

В таблице 7.2 представлено отображение классов функциональных требований безопасности ОО на цели безопасности для ОО.

Таблица 7.2 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

Цели безопасности	Класс ФТБ
O.INSTALL ОО должен быть поставлен, инсталлирован, управляться и функционировать в соответствии с руководствами.	ADO_DEL.1 «Процедуры поставки» ADO_IGS.1 «Процедуры установки, генерации и запуска» AGD_ADM.1 «Руководство администратора» AGD_USR.1 «Руководство пользователя»
O.ACCESS ФБО должны управлять доступом к ресурсам, который основан на идентификаторах пользователей и групп, предоставляемых ОС. ФБО должен разрешать уполномоченным администраторам определять доступность защищаемых ресурсов.	FDP_ACC.1 «Ограниченное управление доступом» FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности» FMT_MSA.1(1) «Управление атрибутами безопасности» FMT_MSA.1(2) «Управление атрибутами безопасности» FMT_MSA.1(3) «Управление атрибутами безопасности» FMT_MSA.1(4) «Управление атрибутами безопасности» FMT_MSA.2 «Безопасные значения атрибутов безопасности» FMT_MSA.3 «Инициализация статических атрибутов» FMT_SMR.1 «Роли безопасности» FPT_RVM.1 «Невозможность обхода ПБО»
O.ACCOUNT ФБО должны обнаруживать попытки несанкционированного доступа к объектам ОО со стороны неуполномоченных на доступ к объектам пользователей.	FAU_GEN.1 (1) «Генерация данных аудита» FAU_GEN.1 (2) «Генерация данных аудита» FAU_GEN.2 «Ассоциация идентификатора пользователя» FAU_STG.1 «Защищенное хранение журнала аудита» FAU_STG.3 «Действия в случае возможной потери данных аудита» FMT_MTD.1(1) «Управление данными ФБО»

Цели безопасности	Класс ФТБ
	FMT_MTD.1(2) «Управление данными ФБО»
O.MANAGE ФБО должны предоставлять все необходимые функции и возможности для поддержки уполномоченных администраторов, ответственных за управление безопасностью ОО.	FMT_MSA.1(1) «Управление атрибутами безопасности» FMT_MSA.1(2) «Управление атрибутами безопасности» FMT_MSA.1(3) «Управление атрибутами безопасности» FMT_MSA.1(4) «Управление атрибутами безопасности» FMT_MSA.2 «Безопасные значения атрибутов безопасности» FMT_MSA.3 «Инициализация статических атрибутов» FMT_MTD.1(1) «Управление данными ФБО» FMT_MTD.1(2) «Управление данными ФБО» FMT_SMR.1 «Роли безопасности»
O.AUTHOR ФБО должны обеспечивать доступ к ОО и его ресурсам только уполномоченным пользователям.	FDP_ACC.1 «Ограниченное управление доступом» FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности» FPT_RVM.1.1 «Невозможность нарушения политики безопасности объекта оценки»
O.AUDITING ФБО должны регистрировать действия пользователей, относящиеся к безопасности ОО, и предоставлять эту информацию уполномоченным администраторам.	FAU_GEN.1 (1) «Генерация данных аудита» FAU_GEN.1 (2) «Генерация данных аудита» FAU_GEN.2 «Ассоциация идентификатора пользователя» FAU_STG.1 «Защищенное хранение журнала аудита» FMT_MTD.1(1) «Управление данными ФБО» FMT_MTD.1(2) «Управление данными ФБО»

Цели безопасности	Класс ФТБ
	FAU_SEL.1 «Избирательный аудит» FAU_SAR.1 «Просмотр аудита» FAU_SAR.1 « Ограниченный просмотр аудита » FAU_SAR.1 «Ограниченный просмотр аудита»
O.SHADOW ФБО должны обеспечивать теневое копирование передаваемых данных, их учет и защиту от несанкционированного доступа при хранении.	FAU_GEN.1 (1) «Генерация данных аудита» FAU_GEN.1 (2) «Генерация данных аудита» FAU_GEN.2 «Ассоциация идентификатора пользователя» FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности» FMT_MTD.1(1) «Управление данными ФБО» FMT_MTD.1(2) «Управление данными ФБО»
O.ENFORCE ФБО должны быть спроектированы и реализованы для обеспечения осуществления политики безопасности организации в предопределенной среде.	ADV_FSP.1 «Неформальная функциональная спецификация» ADV_HLD.1 «Описательный проект верхнего уровня» ADV_RCR.1 «Неформальная демонстрация соответствия»
O.PROTECT ФБО должны защитить файлы настроек ОО, а также данные, необходимые для обеспечения временного доступа к устройствам, от модификации.	FPT_ITT.1 «Базовая защита внутренней передачи данных ФБО»

O.INSTALL ОО должен быть поставлен, инсталлирован, управляться и функционировать в соответствии с руководствами. Компонентом ADO_DEL.1 определены требования к процедуре поставке, компонентом ADO_IGS.1 – к процедурам

инсталляции и настройки. ОО должен эксплуатироваться на основании требований компонентов AGD_ADM.1, AGD_USR.1.

O.ACCESS ОО должен обеспечивать, что только уполномоченные пользователи имеют доступ к объектам ОО. Компонент FDP_ACC.1 определяет политику управления доступом, устанавливающую множество операций субъектов над объектами, взаимодействующих по определенным правилам, установленным компонентом FDP_ACF.1. Администратор уполномочен модифицировать списки управления доступом и, тем самым, определять доступность объектов для субъектов доступа – FMT_MSA.1(1)/FMT_MSA.1(2)/ FMT_MSA.1(3). Компонентом FMT_MSA.3 определено, что защита объектов является непрерывной с момента их создания. Компонент FMT_MSA.2 определяет безопасные значения атрибутов доступа.

O.ACCOUNT ОО должен обеспечивать регистрацию любых неудачных попыток доступа к объектам ОО. Компонентом FAU_GEN.1 определены события, относящиеся к безопасности, которые подвергаются аудиту, указанные события ассоциируются с конкретными пользователями (инициаторами события) – FAU_GEN.2. Хранимые записи аудита защищены от несанкционированного удаления, также обеспечено предотвращение их несанкционированной модификации – FAU_STG.1. Компонентами FMT_MTD.1(1), FMT_MTD.1(2) устанавливается, что управление данными аудита (их удаление) возможно только со стороны администратора.

O.MANAGE ОО должен располагать надлежащими корректно функционирующими средствами администрирования ОО, доступными только уполномоченным администраторам. Согласно компонентам FMT_MSA.1(1)/FMT_MSA.1(2) управление доступом к объектам ОО осуществляется путем модификации атрибутов безопасности политики управления доступом – списков управления доступом (ACL). Модификация списков управления доступом возможна только администратором. Согласно компоненту FMT_MSA.3 (EXT) предусмотрены ограничительные значениями по умолчанию для атрибутов безопасности, используемых в политике управления доступом. Администратор управляет данными аудита – FMT_MTD.1(1)/FMT_MTD.1(2) и списками управления доступом (ACL) –

FMT_MSA.1(1)/FMT_MSA.1(2)/ FMT_MSA.1(3). Компонентом FMT_SMF.1 определены функции управления безопасностью, которые включены в состав ФБО. Компонент FMT_MSA.2 определяет безопасные значения атрибутов доступа.

O.AUTHOR ФБО должны обеспечивать доступ к ОО и его ресурсам только уполномоченным пользователям. Компонент FDP_ACC.1 определяет политику управления доступом, устанавливающую множество операций субъектов над объектами, взаимодействующих по определенным правилам, установленным компонентом FDP_ACF.1. Компонент FPT_RVM.1.1 определяет что бы вызов функций, определяющих ПБО осуществлялся прежде чем разрешалось выполнение других средств безопасности в пределах ОДФ.

O.AUDITING ФБО должны регистрировать действия пользователей, относящиеся к безопасности ОО, и предоставлять эту информацию уполномоченным администраторам. Компонентом FAU_GEN.1 определены события, относящиеся к безопасности, которые подвергаются аудиту, указанные события ассоциируются с конкретными пользователями (инициаторами события) –FAU_GEN.2. Хранимые записи аудита защищены от несанкционированного удаления, также обеспечено предотвращение их несанкционированной модификации – FAU_STG.1. Компонентами FMT_MTD.1(1)/FMT_MTD.1(2) устанавливается, что управление данными аудита (их удаление) возможно только со стороны администратора. Компоненты FAU_SAR задают правила работы с журналами аудита.

O.SHADOW ФБО должны обеспечивать теневое копирование передаваемых данных, их учет и защиту от несанкционированного доступа при хранении. Компанет FAU_GEN.1 определяет требования теневого копирования данных пользователей. Компонент FAU_ GEN.2 связывает данные теневого копирования с идентификатором пользователя. Компонентами FMT_MTD.1(1)/FMT_MTD.1(2) устанавливается, что управление данными аудита (их удаление) возможно только со стороны администратора.

O.ENFORCE ФБО должны быть спроектированы и реализованы для обеспечения осуществления политики безопасности организации в предопределенной

среде. ФБО должны быть разработаны и описаны согласно спецификациям компонентов ADV_FSP.1, ADV_HLD.1, ADV_RCR.1.

O.PROTECT ФБО должны защитить файлы настроек ОО, а также данные, необходимые для обеспечения временного доступа к устройствам, от модификации. Согласно компоненту FPT_ITT.1 ОО обеспечивает защиту от модификации указанных данных, что позволяет предотвратить несанкционированный доступ к контролируемым устройствам и внести несанкционированные изменения в файлы настроек ОО.

7.3.2 Обоснование требований безопасности среды ОО

В таблице 7.3 представлено отображение функциональных требований безопасности среды ОО на цели безопасности для среды.

Таблица 7.3 – Отображение функциональных требований безопасности среды ОО на цели безопасности для среды

Цели безопасности	Функциональные компоненты
OE.ROLE ОС, под управлением которой функционирует ОО, должна обеспечивать надлежащее ассоциирование пользователей с ролями и поддержку роли администратора ОО	FIA_UAU.2 «Аутентификация до любых действий пользователя» FIA_UID.2 «Идентификация до любых действий пользователя» FMT_SMR.1 «Роли безопасности»
OE.TIME ОС, под управлением которой функционирует ОО, должна обеспечивать предоставление надлежащего источника меток времени, в том числе и для ОО	FPT_STM.1 «Надежные метки времени»

Цели безопасности	**Функциональные компоненты**
OE.CONFIG ОС, под управлением которой функционирует ОО, должна устанавливаться, конфигурироваться и управляться согласно руководств, обеспечивая уникальные идентификаторы пользователей, и настройки, защищающие ОО от несанкционированного доступа	FIA_ATD.1 «Определение атрибутов пользователя» FIA_UID.2 «Идентификация до любых действий» ADO_IGS.1 «Процедуры установки, генерации и запуска» AGD_ADM.1 «Руководство администратора»
OE.IDENTITY ОС, под управлением которой функционирует ОО, должна обеспечивать надлежащие механизмы идентификации субъектов доступа к ОО	FIA_ATD.1 «Определение атрибутов пользователя» FIA_UID.2 «Идентификация до любых действий»
OE.AUTHENT ОС, под управлением которой функционирует ОО, должна обеспечивать надлежащие механизмы аутентификации субъектов доступа к ОО, позволяющие защитить аутентификационную информацию и ОО от прямых или умышленных атак нарушителя с умеренным потенциалом нападения.	FIA_ATD.1 «Определение атрибутов пользователя» FIA_UID.2 «Идентификация до любых действий» FIA_UAU.2 Аутентификация до любых действий пользователя FIA_AFL.1 «Обработка отказов аутентификации» FIA_SOS.1 «Верификация секретов» FPT_RVM.1 «Невозможность обхода ПБО»

Цели безопасности	Функциональные компоненты
OE.RECOVER ОС, под управлением которой функционирует ОО, должна предусматривать процедуры и механизмы безопасного восстановления ОО после сбоев (отказов) программного и аппаратного обеспечения, а также других прерываний функционирования	FPT_FLS.1 «Доступность передаваемых данных комплекса средств безопасности»
OE.PROTECT Все программное, аппаратное обеспечение и периферийное оборудование, взаимодействующее с ОО, должно быть доверенным, защищенным от несанкционированного физического доступа и не должно содержать угроз безопасности обрабатываемой и передаваемой информации	-
OE.COPY_REC Для безопасного функционирования ОО должно быть организовано резервное копирование БД с периодичностью, обеспечивающий возможность их восстановления в случае фатального разрушения БД	AGD_ADM.1 «Руководство администратора»

OE.ROLE Операционной системой, под управлением которой функционирует ОО, должно быть обеспечено надлежащее ассоциирование пользователей с ролями и поддержка административной роли. Согласно компоненту (FMT_SMR.1) операционная система поддерживает роль администратора и способна ассоциировать пользователей с данной ролью, предварительно проведя процедуры идентификации (FIA_UID.2) и аутентификации (FIA_UAU.2).

OE.TIME Должно быть обеспечено предоставление для ОО надлежащего источника меток времени. Операционная система предоставляет для ОО надежные метки времени (FPT_STM.1).

OE.CONFIG Безопасная установка ОС, под которой работает ОО, должна проводиться в соответствии с существующими руководствами (ADO_IGS.1, AGD_ADM.1) по безопасной установке и эксплуатации ОО. Кроме этого, идентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО. Согласно компоненту (FIA_ATD.1) для каждого пользователя, в качестве атрибутов безопасности, операционной системой поддерживаются идентификатор пользователя и идентификатор группы. Пользователи идентифицируются до выполнения ими каких-либо действий с ОО (FIA_UID.2).

OE.IDENTIFY Идентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО. Согласно компоненту (FIA_ATD.1) для каждого пользователя, в качестве атрибутов безопасности, операционной системой поддерживаются идентификатор пользователя и идентификатор группы. Пользователи идентифицируются до выполнения ими каких-либо действий с ОО (FIA_UID.2).

OE.AUTHENT До выполнения субъектами каких-либо действий с ОО производится их аутентификация (FIA_UAU.2), где в качестве атрибутов безопасности (FIA_ATD.1) ОС поддерживаются идентификатор пользователя и идентификатор группы. Далее производится их идентификация (FIA_UID.2).

OE.RECOVER ОС, под управлением которой функционирует ОО, должна обладать механизмами безопасного восстановления ОО после сбоев (отказов) программного и аппаратного обеспечения (FPT_FLS.1).

OE.PROTECT Данная задача реализуется организационными мерами.

OE.COPY_REC Данная задача реализуется организационными мерами, где администратор должен руководствоваться документацией производителя (AGD_ADM.1).

7.3.3 Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ЗБ соответствуют ОУД2 и выбраны, исходя из необходимости независимого подтверждения уровня доверия, достаточного для обработки конфиденциальной информации, и нецелесообразности для разработчика прилагать усилия для превышения обычных практических коммерческих требований.

Выбор ОУД2 в качестве основы требований доверия в настоящем ЗБ является достаточным при определении допустимости использования ОО для обработки конфиденциальной информации.

7.4 Обоснование зависимости требований

В таблице 7.4 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворяются в настоящем ЗБ либо включением компонентов, определенных в части 2 ОК под рубрикой «Зависимости», либо включением компонентов, более высоких в иерархии по отношению к компонентам, определенным в части 2 ОК под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 7.4 является справочным и содержит компоненты, определенные в части 2 ОК в описании компонентов требований, приведенных в столбце 1 таблицы 7.4, под рубрикой «Зависимости».

Столбец 3 таблицы 7.4 показывает, какие компоненты требований были реально включены в настоящий ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 7.4. Компоненты требований в столбце 3 таблицы 7.4 либо совпадают с компонентами в столбце 2 таблицы 7.4, либо иерархичны по отношению к ним.

Для компонента FMT_MSA.2 зависимостью от компонента ADV_SPM.1 «Неформальная модель политики безопасности ОО» для ОУД2 согласно части 2 ОК можно пренебречь, т.к. разработчик в документации к ОО привел полное описание безопасных значений атрибутов безопасности.

Таблица 7.4 – 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.2
FAU_STG.1	FAU_GEN.1	FAU_GEN.1

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_GEN.1 FAU_SAR.1	FAU_GEN.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
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1], FMT_MSA.2, FMT_SMR.1	FDP_ACC.1, FMT_MSA.2, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1 [FDP_ACC.1 или FDP_IFC.1], FMT_MSA.1, FMT_SMR.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1, FMT_MSA.3
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
Зависимости функциональных требований среды ИТ		
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2

7.5 Обоснование краткой спецификации ОО

Обоснование краткой спецификации ОО представлено таблицами 7.5 и 7.6.

Таблица 7.5 – Отображение функциональных требований безопасности на функции безопасности

Функциональные требования безопасности	Функции безопасности
FAU_GEN.1 (1), FAU_STG.3	АУ1, АУ2
FAU_GEN.1 (2), FAU_GEN.2	АУ2

FAU_SAR.1	УД.1, АУ.4
FAU_SAR.2	УД.1,
FAU_SAR.3	АУ.5
FAU_SEL.1	АУ2
FAU_STG.1	АУ3
FDP_ACC.1	УД.1
FDP_ACF.1	УД.1
FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3)	УД.2
FMT_MSA.1(4)	УД.4
FMT_MSA.2, FMT_MSA.3	УД.3, УД.5
FMT_MTD.1(1), FMT_MTD.1(2)	УБ.1 УБ.3
FPT_RVM.1	УБ.4
FMT_SMR.1	УБ.1, УБ.2, УБ.3
FTP_ITT.1	ЗФ.1

Таблица 7.6 – Отображение требования доверия на меры доверия к безопасности ОО

Мера доверия	**Требование доверия**	**Название компонента доверия**
Управление конфигурацией	ACM_CAP.2	Элементы конфигурации
Поставка и эксплуатация	ADO_DEL.1	Процедуры поставки
	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_HLD.1	Описательный проект верхнего уровня
	ADV_RCR.1	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_COV.1	Свидетельство покрытия
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО
	AVA_VLA.1	Анализ уязвимостей разработчиком