ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России
30 декабря 2013 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ ЗАГРУЗОЧНОЙ ЗАПИСИ ШЕСТОГО КЛАССА ЗАЩИТЫ

ИТ.СДЗ.З3б.ПЗ

2013

Содержание

Перечень сокращений

ЗБ – задание по безопасности
ИС – информационная система
ИТ – информационная технология
ОО – объект оценки
ОУД – оценочный уровень доверия
ПБО – политика безопасности объекта оценки
ПЗ – профиль защиты
ПО – программное обеспечение
СВТ – средство вычислительной техники
СДЗ – средство доверенной загрузки
УК – управление конфигурацией
ФБО – функции безопасности объекта оценки
ФТБ – функциональные требования безопасности

1. Общие положения

Настоящий методический документ ФСТЭК России разработан и утвержден в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и предназначен для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации (далее – разработчики), заявителей на осуществление сертификации продукции (далее – заявители), а также испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям по безопасности информации (далее – оценщики) при проведении ими работ по сертификации средств доверенной загрузки (СДЗ) на соответствие Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 г. № 119 (зарегистрирован в Минюсте России, регистрационный № 30604 от 16 декабря 2013 г.).

Настоящий методический документ ФСТЭК России детализирует и определяет взаимосвязи требований к функциям безопасности СДЗ, установленным Требованиями к средствам доверенной загрузки, утвержденными приказом ФСТЭК России от 27 сентября 2013 г. № 119.

Профиль защиты разработан в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

1.1. Введение профиля защиты

Данный раздел содержит информацию общего характера. Подраздел «Идентификация профиля защиты» предоставляет маркировку и описательную информацию, которые необходимы, чтобы контролировать и идентифицировать профиль защиты (ПЗ) и объект оценки (ОО), к которому он относится. Подраздел «Аннотация профиля защиты» содержит общую характеристику ПЗ, позволяющую определить применимость ОО, к которому относится настоящий ПЗ, в конкретной ситуации. В подразделе «Соглашения» дается описание операций конкретизации компонентов требований безопасности средств доверенной загрузки. В подразделе «Термины и определения» представлены определения основных терминов, специфичных для данного ПЗ. В подразделе «Организация профиля защиты» дается пояснение организации документа.

1.2. Идентификация профиля защиты

Название ПЗ: Профиль защиты средства доверенной загрузки уровня загрузочной записи шестого класса защиты.

Тип СДЗ: СДЗ уровня загрузочной записи.

Класс защиты:	Шестой.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.СДЗ.3У6.ПЗ.
Идентификация ОО:	СДЗ уровня загрузочной записи жесткого диска.
Уровень доверия:	Оценочный уровень доверия 1 (ОУД1), усиленный компонентом AVA_SOF.1 «Оценка стойкости функции безопасности объекта оценки», расширенный компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства доверенной загрузки».
Идентификация:	Требованиями к средствам доверенной загрузки, утвержденными приказом ФСТЭК России от 27 сентября 2013 г. № 119. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
Ключевые слова:	Средства доверенной загрузки, ОУД1.

1.3. Аннотация профиля защиты

Настоящий ПЗ определяет требования безопасности для средств доверенной загрузки уровня загрузочной записи жесткого диска (объекта оценки).

Объект оценки представляет собой программно-техническое средство, которое предназначено для предотвращения несанкционированного доступа к ресурсам информационной системы при загрузке нештатной операционной среды функционирования и загрузке с нештатного загрузочного диска.

Объект оценки должен обеспечивать нейтрализацию следующих угроз безопасности информации:

несанкционированного доступа к информации за счет загрузки нештатной операционной системы и обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы;

несанкционированной загрузки штатной операционной системы и получение несанкционированного доступа к информации;

несанкционированного изменения конфигурации (параметров) средства доверенной загрузки;

преодоления или обхода функций безопасности средств доверенной загрузки.

В СДЗ уровня загрузочной записи жесткого диска должны быть реализованы следующие функции безопасности:

разграничение доступа к управлению средством доверенной загрузки;

аудит безопасности средства доверенной загрузки;

идентификация и аутентификация;

управление доступом к ресурсам средства вычислительной техники.

В среде, в которой функционирует СДЗ, должны быть реализованы следующие функции безопасности среды:

физическая защита средств вычислительной техники, доступ к которым контролируется с применением средств доверенной загрузки;

обеспечение условий безопасного функционирования (расширенные возможности аудита безопасности);

управление атрибутами безопасности компонентов средств доверенной загрузки;

защита от отключения (обхода).

Функции безопасности СДЗ уровня загрузочной записи жесткого диска должны обладать составом функциональных возможностей (функциональных требований безопасности), обеспечивающих реализацию этих функций.

В ПЗ изложены следующие виды требований безопасности, предъявляемые к СДЗ уровня загрузочной записи жесткого диска:

функциональные требования безопасности;

требования доверия к безопасности.

Функциональные требования безопасности СДЗ, изложенные в ПЗ, включают:

требования к защите остаточной информации;

требования по управлению режимами выполнения функций безопасности СДЗ (работой СДЗ);

требования по разграничению доступа к управлению СДЗ;

требования по управлению данными функций безопасности (данными СДЗ);

требования по управлению ролями субъектов;

требования по управлению доступом к ресурсам СВТ;

требования к аутентификации и идентификации;

требования к аудиту функционирования СДЗ.

Функциональные требования безопасности для СДЗ уровня загрузочной записи жесткого диска выражены на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408–2.

Состав функциональных требований безопасности (ФТБ), включенных в настоящий ПЗ, обеспечивает следующие функциональные возможности СДЗ уровня загрузочной записи жесткого диска:

возможность определения действий при превышении 10 или устанавливаемого администратором СДЗ количества неуспешных попыток аутентификации пользователя в пределах от 1 до 10;

идентификация и аутентификация пользователя до выполнения основных действий по загрузке операционной системы или администратора до выполнения действий по управлению средством доверенной загрузки;

исключение отображения действительного значения аутентификационной информации при ее вводе пользователем в диалоговом интерфейсе;

обеспечение доступности ресурсов средства вычислительной техники с штатной операционной системой, данными пользователя в случае положительной аутентификации пользователя;

обеспечение недоступности штатными средствами ресурсов средства вычислительной техники с штатной операционной системой, данными пользователя в случае загрузки нештатной операционной системы;

возможность со стороны администраторов СДЗ управлять данными (данными средства доверенной загрузки), в том числе атрибутами безопасности, используемыми функциями безопасности средства доверенной загрузки;

поддержка определенных ролей (учетных записей пользователей) для средства доверенной загрузки и их ассоциации с конкретными администраторами средства доверенной загрузки и пользователями информационной системы.

Требования доверия к безопасности СДЗ сформированы на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408–3 и специальных компонентов.

Требования доверия к безопасности СДЗ образуют оценочный уровень доверия 1 (ОУД1), усиленный компонентами AVA_SOF.1 «Оценка стойкости функции безопасности объекта оценки» и расширенный компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства доверенной загрузки».

В целях обеспечения условий для безопасного функционирования СДЗ в настоящем ПЗ определены цели и требования для среды функционирования СДЗ. Эксплуатационная документация на СДЗ должна содержать четкие указания по реализации и порядку оценки реализации всех функций безопасности среды функционирования СДЗ.

1.4. Соглашения

ГОСТ Р ИСО/МЭК 15408 допускает выполнение определенных операций над требованиями безопасности. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

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

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

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

В настоящем ПЗ используются компоненты требований безопасности, включающие частично выполненные операции **«назначение»** и предполагающие завершение операций в задании по безопасности (ЗБ). В данных компонентах незавершенная часть операции **«назначение»** обозначается как [назначение: *область предполагаемых значений*].

В настоящем ПЗ используются компоненты требований безопасности, включающие незавершенные операции **«назначение»,** в которых область предполагаемых значений уточнена по отношению к исходному компоненту из ГОСТ Р ИСО/МЭК 15408. В данных компонентах операции **«назначение»** с уточненной областью предполагаемых значений обозначаются как [назначение: ***уточненная область предполагаемых значений***].

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

В настоящий ПЗ включен ряд требований безопасности, сформулированных в явном виде. Краткая форма имен компонентов требований, сформулированных в явном виде, содержит текст (EXT).

Замечания по применению предназначены либо для разъяснения назначения некоторого требования, идентификации вариантов реализации, либо для определения условий выполнения требования. В случае использования замечания по применению следуют за компонентом требования.

Настоящий профиль защиты содержит ряд незавершенных операций над компонентами функциональных требований безопасности. Эти операции должны быть завершены в задании по безопасности на конкретную реализацию СДЗ уровня базовой системы ввода-вывода.

1.5. Термины и определения

В настоящем ПЗ применяются следующие термины с соответствующими определениями.

Администратор СДЗ – уполномоченная роль, ответственная за установку, администрирование и эксплуатацию ОО (СДЗ).

Внутренний нарушитель – пользователь (субъект) информационной системы, действия которого направлены на нарушение безопасности информации в информационной системе.

Внешний нарушитель – лицо (субъект), не являющееся пользователем информационной системы, и действия которого направлены на нарушение безопасности информации в информационной системе.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО (конкретного СДЗ).

Объект оценки – подлежащее сертификации (оценке) СДЗ с руководствами по эксплуатации.

Политика безопасности ОО – совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых СДЗ.

Профиль защиты – совокупность требований безопасности для СДЗ.

Средство доверенной загрузки – программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, контроль целостности своего программного обеспечения и среды функционирования (программной среды и аппаратных компонентов средств вычислительной техники), а также не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы.

Угроза безопасности информации – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.

Функции безопасности ОО – совокупность всех функций безопасности СДЗ, направленных на осуществление политики безопасности объекта оценки (ПБО).

1.6. Организация профиля защиты

Раздел 1 «Введение профиля защиты» содержит информацию управления документооборотом и описательную информацию, необходимые для идентификации ПЗ и ОО, к которому он относится.

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

Раздел 3 «Среда безопасности объекта оценки» содержит описание решаемой с использованием СДЗ проблемы безопасности. В данном разделе определяется совокупность угроз безопасности, политика безопасности организации и предположения безопасности (обязательные условия безопасного использования ОО).

В разделе 4 «Цели безопасности» определена совокупность целей (задач) безопасности для СДЗ и среды функционирования СДЗ.

В разделе 5 «Требования безопасности» на основе ГОСТ Р ИСО/МЭК 15408–2 и ГОСТ Р ИСО/МЭК 15408–3 определены, соответственно, функциональные требования безопасности ИТ и требования доверия к безопасности ОО.

В Разделе 6 «Обоснование» демонстрируется, что ПЗ определяет полную и взаимосвязанную совокупность требований безопасности ИТ, а ОО решает проблему безопасности, изложенную в разделе ПЗ «Среда безопасности объекта оценки».

2. Описание объекта оценки

2.1. Тип изделия информационных технологий

Объектом оценки в настоящем ПЗ является средство доверенной загрузки уровня загрузочной записи.

Объект оценки представляет собой программно-техническое средство, которое предназначено для предотвращения несанкционированного доступа к ресурсам информационной системы при загрузке нештатной операционной среды функционирования и загрузке с нештатного загрузочного диска.

2.2. Основные функциональные возможности объекта оценки

В данном подразделе представлено краткое описание функциональных возможностей ОО.

Средства доверенной загрузки, соответствующие настоящему ПЗ, должны обеспечивать:

возможность определения действий при превышении 10 или устанавливаемого администратором СДЗ количества неуспешных попыток аутентификации пользователя в пределах от 1 до 10;

идентификацию и аутентификацию пользователя до выполнения основных действий по загрузке операционной системы или администратора СДЗ до выполнения действий по управлению средством доверенной загрузки;

исключение отображения действительного значения аутентификационной информации при ее вводе пользователем в диалоговом интерфейсе;

доступность ресурсов средства вычислительной техники с штатной операционной системой, данными пользователя в случае положительной аутентификации пользователя;

недоступность штатными средствами ресурсов средства вычислительной техники с штатной операционной системой, данными пользователя в случае загрузки нештатной операционной системы;

возможность со стороны администраторов управлять данными (данными средства доверенной загрузки), используемыми функциями безопасности средства доверенной загрузки;

поддержку определенных ролей (учетных записей пользователей) для средства доверенной загрузки и их ассоциации с конкретными администраторами средства доверенной загрузки и пользователями информационной системы.

СДЗ уровня загрузочной записи предназначены для осуществления сокрытия сведений о структуре и размещении разделов жесткого диска путем реализации следующих процессов:

получения управления до загрузки штатной операционной системы;

идентификации и аутентификации пользователя;

обеспечения доступности разделов жесткого диска (или другого соответствующего носителя) со штатной операционной системой, данными пользователя и иной информацией в случае положительной аутентификации пользователя с последующей загрузкой штатной операционной системы;

блокировки загрузки в случае превышения числа неудачных попыток аутентификации пользователя;

обеспечения недоступности штатными средствами операционной системы разделов жесткого диска (или другого соответствующего носителя) со штатной операционной системой, данными пользователя и другой информацией в случае загрузки нештатной операционной системы;

регистрации событий безопасности и записи информации аудита в выделенную область памяти в среде функционирования.

3. Среда безопасности объекта оценки

Данный раздел содержит описание следующих аспектов решаемой с использованием СДЗ проблемы безопасности:

предположений безопасности (обязательных условий безопасного использования ОО);

угроз безопасности, которым должен противостоять ОО и среда функционирования ОО;

политики безопасности организации, которую должен выполнять ОО.

3.1. Предположения безопасности

Предположения относительно предопределенного использования ОО

Предположение-1

Должны быть обеспечены условия совместимости ОО с СВТ для реализации своих функциональных возможностей.

Предположение-2

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с эксплуатационной документацией.

Предположения, связанные с защитой ОО

Предположение-3

Должна быть обеспечена невозможность осуществления действий, направленных на нарушение физической целостности СВТ, доступ к которым контролируется с применением СДЗ.

Предположение-4

Должен быть обеспечен надежный источник меток времени для записи событий аудита безопасности СДЗ.

Предположение-5

Должна быть обеспечена невозможность отключения (обхода) компонентов ОО.

Предположение, имеющее отношение к персоналу

Предположение-6

Персонал, ответственный за функционирование ОО, должен обеспечивать функционирование ОО в соответствии с эксплуатационной документацией.

3.2. Угрозы безопасности информации

3.2.1. Угрозы, которым должен противостоять ОО

В настоящем ПЗ определена следующая угроза, которой необходимо противостоять средствами ОО.

Угроза-1

1. Аннотация угрозы – несанкционированный доступ к информации за счет загрузки нештатной операционной системы и обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – попытки несанкционированной загрузки нештатной операционной системы с использованием носителей информации.

4. Используемые уязвимости – наличие в составе СВТ устройств для подключения носителей информации с нештатной операционной системой; отсутствие или недостатки механизмов обеспечения недоступности штатными средствами операционной системы разделов жесткого диска (или другого соответствующего носителя) со штатной операционной системой, данными пользователя и другими информационными ресурсами в случае загрузки нештатной операционной системы.

5. Вид информационных ресурсов, потенциально подверженных угрозе – разделы жесткого диска (или другого соответствующего носителя) со штатной операционной системой, данными пользователя и другими информационными ресурсами.

6. Нарушаемые свойства безопасности информационных ресурсов – недоступность.

7. Возможные последствия реализации угрозы – несанкционированный доступ к информации пользователей СВТ и ИС; нарушение режимов функционирования СВТ и ИС.

Угроза-2

1. Аннотация угрозы – несанкционированная загрузка штатной операционной системы и получение несанкционированного доступа к информации.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – осуществление несанкционированной загрузки штатной операционной системы.

4. Используемые уязвимости – недостатки механизмов идентификации, аутентификации, управления доступом штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы.

5. Вид информационных ресурсов, потенциально подверженных угрозе – атрибуты безопасности субъектов и объектов доступа, правила управления доступом субъектов к объектам доступа.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Возможные последствия реализации угрозы – несанкционированный доступ к информации пользователей СВТ и ИС; нарушение режимов функционирования СВТ и ИС.

Угроза-3

1. Аннотация угрозы – несанкционированное изменение конфигурации (параметров) СДЗ.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированный доступ к конфигурационной информации (настройкам) СДЗ.

4. Используемая уязвимость – недостатки процедур разграничения полномочий в ИС, уязвимости технических, программных и программно-технических средств ИС, которые взаимодействуют с СДЗ и могут влиять на функционирование СДЗ, недостатки механизмов управления доступом.

5. Вид информационных ресурсов, потенциально подверженных угрозе – настройки программного обеспечения СДЗ.

6. Нарушаемые характеристики безопасности информационных ресурсов – целостность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования СДЗ.

Угроза-4

1. Аннотация угрозы – преодоление или обход функций СДЗ, идентификация/аутентификация за счет недостаточного качества аутентификационной информации.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – преодоление или обход функций СДЗ идентификация/аутентификация.

4. Используемая уязвимость – недостатки механизмов идентификации/аутентификации.

5. Вид информационных ресурсов, потенциально подверженных угрозе – ресурсы ИС.

6. Нарушаемые характеристики безопасности информационных ресурсов – конфиденциальность, доступность.

7. Возможные последствия реализации угрозы – несанкционированный доступ к информации ИС.

3.2.2. Угрозы, которым противостоит среда

В настоящем ПЗ определены следующие угрозы, которым должна противостоять среда функционирования ОО.

Угроза среды-1

1. Аннотация угрозы – отключение (обход) или блокирование СДЗ.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированный доступ к СДЗ с использованием штатных и нештатных средств, в том числе удаленно (по сети).

4. Используемые уязвимости – недостатки механизмов управления доступом, физическая защита СВТ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – данные функций безопасности СДЗ.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Возможные последствия реализации угрозы – неэффективность работы СДЗ.

Угроза среды-2

1. Аннотация угрозы – нарушение целостности ПО СДЗ.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированный доступ к СДЗ с использованием штатных и нештатных средств.

4. Используемые уязвимости – недостатки механизмов управления доступом, физической защиты оборудования ИС; недостатки механизмов защиты журналов аудита СДЗ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – ПО СДЗ, данные СДЗ.

6. Нарушаемые свойства безопасности информационных ресурсов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования СДЗ.

3.3. Политика безопасности организации

Объект оценки должен выполнять приведенные ниже правила политики безопасности организации.

Политика безопасности-1

Объект оценки должен быть защищен от несанкционированного доступа и нарушений в отношении функций и данных ОО.

Политика безопасности-2

Управление параметрами СДЗ, которые влияют на выполнение функций безопасности СДЗ, должно осуществляться только уполномоченными администраторами СДЗ.

Политика безопасности-3

Должна быть обеспечена возможность доступа к информационным ресурсам в случае успешной проверки подлинности операционной системы.

Политика безопасности-4

Объект оценки должен осуществлять механизмы идентификации и аутентификации.

4. Цели безопасности

4.1. Цели безопасности для объекта оценки

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Разграничение доступа к управлению СДЗ

Объект оценки должен обеспечивать разграничение доступа к управлению СДЗ на основе ролей администраторов СДЗ.

Цель безопасности-2

Управление параметрами СДЗ

Объект оценки должен обеспечить возможность управления параметрами СДЗ, которые влияют на выполнение функций безопасности СДЗ, со стороны администраторов СДЗ.

Цель безопасности-3

Доступ к данным

Объект оценки должен обеспечить доступ к разделам жесткого диска (или другого соответствующего носителя) со штатной операционной системой, данными пользователя и другими информационными ресурсами в случае успешной проверки подлинности операционной системы с использованием ФБ СДЗ.

Обеспечение недоступности штатными средствами операционной системы разделов жесткого диска (или другого соответствующего носителя) со штатной операционной системой, данными пользователя и другими информационными ресурсами в случае загрузки нештатной операционной системы.

Цель безопасности-4

Идентификация и аутентификация

Объект оценки должен обеспечивать ассоциации пользователей с соответствующими атрибутами безопасности.

4.2. Цели безопасности для среды

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

Цель для среды функционирования ОО-1

Совместимость

Объект оценки должен быть совместим с СВТ, в котором он функционирует.

Цель для среды функционирования ОО-2

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление объектом оценки в соответствии с эксплуатационной документацией.

Цель для среды функционирования ОО-3

Физическая защита ОО

Объект оценки должен быть расположен в пределах контура средств контроля доступа, которые предотвращают неправомочный физический доступ со стороны посторонних лиц.

Цель для среды функционирования ОО-4

Защита данных ФБО

Должна быть обеспечена защищенная область для выполнения функций безопасности СДЗ.

Цель для среды функционирования ОО-5

Поддержка аудита

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

Цель для среды функционирования ОО-6

Обеспечение условий безопасного функционирования

Отсутствие в среде функционирования объекта оценки в составе системного ПО и прикладного ПО средств для перезаписи (перепрограммирования) СДЗ. Обеспечение невозможности отключения (обхода) компонентов СДЗ.

Цель для среды функционирования ОО-7

Требования к персоналу

Персонал, ответственный за функционирование объекта оценки, должен обеспечивать надлежащее функционирование объекта оценки, руководствуясь исключительно эксплуатационной документацией.

5. Требования безопасности

В данном разделе ПЗ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из ГОСТ Р ИСО/МЭК 15408–2. Требования доверия основаны на компонентах требований доверия из ГОСТ Р ИСО/МЭК 15408–3 и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД1, усиленного компонентом AVA_SOF.1 «Оценка стойкости функции безопасности объекта оценки» и расширенного компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства доверенной загрузки». Требование безопасности AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства доверенной загрузки» сформулировано в явном виде (расширение ГОСТ Р ИСО/МЭК 15408–3).

5.1. Требования безопасности для объекта оценки

5.1.1. Функциональные требования безопасности ОО

Функциональные компоненты из ГОСТ Р ИСО/МЭК 15408–2, на которых основаны функциональные требования безопасности ОО, а также компоненты сформулированных в явном виде расширенных требований приведены в таблице 5.1.

Таблица 5.1

Функциональные компоненты, на которых основаны ФТБ ОО

Компонент	Название компонента
FIA_AFL.1	Обработка отказов аутентификации
FIA_UAU.1	Выбор момента аутентификации
FIA_UID.1	Выбор момента идентификации
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FMT_SMF.1	Спецификация функций управления
FMT_MTD.1	Управление данными функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_SMR.1	Роли безопасности

5.1.1.1. Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику управления доступом к ресурсам средства вычислительной техники] для

[а) субъектов доступа: пользователи; процессы, запущенные от имени пользователей;

б) объектов доступа: ресурсы СВТ со штатной ОС, данными пользователей;

в) операций субъектов на объектах: доступность (в соответствии с правилами разграничения доступа); недоступность].

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 ресурсам средства вычислительной техники] к объектам, основываясь на [выбор: идентификаторы пользователей, [назначение: ***другие*** *атрибуты безопасности, именованные группы атрибутов безопасности*]].

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

[а) доступность ресурсов средства вычислительной техники со штатной операционной системой, данными пользователями, если результат аутентификации пользователя – положительный;

б) недоступность ресурсов средства вычислительной техники со штатной операционной системой, данными пользователями, если результат аутентификации пользователя – отрицательный].

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

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

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

Замечания по применению: Разработчик ЗБ FDP_ACF.1.1 может ограничить список атрибутов безопасности идентификаторами пользователями и (или) использовать (в соответствии с FMT_MSA.3) другие атрибуты безопасности.

5.1.1.2. Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [выбор: [десять], *устанавливаемое администратором* **СДЗ** *положительное целое число в пределах* [от 1 до 10]] неуспешных попыток аутентификации, относящихся к [назначение: *список событий аутентификации*].

FIA_AFL.1.2 При достижении или превышении **установленного в FIA_AFL.1.1** числа неуспешных попыток аутентификации ФБО должны выполнить [назначение: *список действий*].

Зависимости: FIA_UAU.1 «Выбор момента аутентификации».

FIA_UAU.1Выбор момента аутентификации

FIA_UAU.1.1 ФБО должны допускать выполнение [назначение: *список действий, выполняемых при посредничестве ФБО*] от имени пользователя прежде, чем пользователь аутентифицирован.

FIA_UAU.1.2 ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Зависимости: FIA_UID.1 «Выбор момента идентификации».

FIA_UID.1 Выбор момента идентификации

FIA_UID.1.1 ФБО должны допускать [назначение: *перечень действий, выполняемых при посредничестве ФБО*] от имени пользователя прежде, чем он идентифицирован.

FIA_UID.1.2 ФБО должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Зависимости отсутствуют.

5.1.1.3. Управление безопасностью (FMT)

FMT_SMF.1 Спецификация функций управления

FMT_SMF.1.1 ФБО должны быть способны к выполнению следующих функций управления безопасностью: [управление режимом выполнения функций безопасности, управление данными ФБО, управление атрибутами безопасности].

Зависимости отсутствуют.

FMT_MTD.1 Управление данными ФБО

FMT_MTD.1.1 ФБО должны **ограничить** возможность [выбор: *изменение значений по умолчанию, запрос, модификация, удаление, очистка,* [назначение: *другие операции*]] следующих данных [назначение: *список данных ФБО*] только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 «Роли безопасности»,

FMT_SMF.1 «Спецификация функций управления».

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления атрибутами безопасности], предоставляющую возможность [выбор: *изменять значения по умолчанию, запрашивать, модифицировать, удалять,* [назначение: *другие операции*]] атрибуты безопасности [выбор: идентификаторы пользователей, [назначение: *список **других** атрибутов безопасности*] только [*назначение: уполномоченные идентифицированные роли*].

Зависимости: [FDP_ACC.1 «Ограниченное управление доступом» или
FDP_IFC.1 «Ограниченное управление информационными потоками»],
FMT_SMR.1 «Роли безопасности»,
FMT_SMF.1 «Спецификация функций управления».

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику управления атрибутами безопасности], предусматривающую [выбор (выбрать одно из): *ограничительные, разрешающие, другие свойства*] значений по умолчанию для атрибутов безопасности, которые используются для осуществления **политики управления атрибутами безопасности**.

FMT_MSA.3.2 ФБО должны позволять [назначение: *уполномоченные идентифицированные роли*] 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».

Замечания по применению: В FMT_MSA.3.2 «объект или информация» следует трактовать как ресурс СВТ, на базе которого создаются объекты хранения штатной ОС и данных пользователей.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли [
а) администратор СДЗ;
б) пользователь,
[назначение: другие *уполномоченные идентифицированные роли*]].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать пользователей с ролями.

Зависимости: FIA_UID.1 «Выбор момента идентификации».

Замечания по применению: Конкретизация данного требования определяет различные роли, которые ФБО следует распознавать.

5.1.2. Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из ГОСТ Р ИСО/МЭК 15408–3 и образуют ОУД1, усиленный компонентом AVA_SOF.1 «Оценка стойкости функции безопасности объекта оценки» и расширенный компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства доверенной загрузки» (см. таблицу 5.2).

Таблица 5.2

Требования доверия к безопасности ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Управление конфигурацией	ACM_CAP.1	Номера версий
Поставка и эксплуатация	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_RCR.1	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО
Обновление СДЗ	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность средства доверенной загрузки

5.1.2.1. Управление конфигурацией (ACM)

ACM_CAP.1 Номера версий

Зависимости отсутствуют.

Элементы действий разработчика

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

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

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

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

5.1.2.2. Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Зависимости

AGD_ADM.1 Руководство администратора.

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

Зависимости

ADV_RCR.1 Неформальная демонстрация соответствия.

Элементы действий разработчика

ADV_FSP.1.1D Разработчик (заявитель) должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

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

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

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

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

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

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

ADV_RCR.1 Неформальная демонстрация соответствия

Зависимости отсутствуют.

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

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация.

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 **и четкие указания по реализации и порядку оценки реализации всех функций безопасности среды функционирования ОО**.

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

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация.

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

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

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

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

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

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

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

Элементы действий оценщика

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

5.1.2.5. Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ATE_FUN.1 Функциональное тестирование.

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

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

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

5.1.2.6. Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ADV_HLD.1 Описательный проект верхнего уровня.

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

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.

5.1.2.7. Требования к ОО, сформулированные в явном виде

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность средства доверенной загрузки

Элементы действий заявителя (разработчика, производителя)

AMA_SIA_EXT.3.1D Заявитель (разработчик, производитель) должен представить материалы анализа влияния обновлений на безопасность средства доверенной загрузки.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность средства доверенной загрузки должны

содержать краткое описание влияния обновлений на задание по безопасности, функции безопасности средства доверенной загрузки или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.3.2C Материалы анализа влияния обновлений на безопасность средства доверенной загрузки для обновлений, влияющих на безопасность, должны идентифицировать функции безопасности, компоненты средства доверенной загрузки, на которые влияет данное обновление.

Элементы действий испытательной лаборатории

AMA_SIA_EXT.3.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению документированных материалов.

AMA_SIA_EXT.3.2E Испытательная лаборатория должна подтвердить влияние (отсутствие влияния) обновлений на безопасность средства доверенной загрузки.

5.2. Требования безопасности для среды информационных технологий

Функциями безопасности, реализуемыми средой ИТ в интересах обеспечения безопасности ОО, являются функции«Поддержка аудита» и «Защита данных ФБО».

Функциональные компоненты из ГОСТ Р ИСО/МЭК 15408–2, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.3.

Таблица 5.3

Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FPT_STM.1	Надежные метки времени

5.2.1. Управление безопасностью (FMT)

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБ среды функционирования должны быть способны предоставлять надежные метки времени для собственного использования.

Зависимости отсутствуют.

Замечания по применению: Представленные в данном подразделе требования могут быть реализованы как программно-техническими средствами в среде функционирования СДЗ, так и самим СДЗ или совместно СДЗ и средой ИТ.

6. Обоснование

В данном разделе дано логическое обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ПЗ.

6.1. Обоснование целей безопасности

6.2.1. Обоснование целей безопасности для ОО

В таблице 6.1 приведено отображение целей безопасности для ОО на угрозы и политику безопасности организации.

Таблица 6.1

Отображение целей безопасности для ОО на угрозы и политику безопасности организации

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4
Угроза-1	X			
Угроза-2	X			
Угроза-3		X		
Угроза-4			X	
Политика безопасности-1	X			
Политика безопасности-2		X		
Политика безопасности-3			X	
Политика безопасности-4				X

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-1**, так как обеспечивает возможность разграничения доступа к СДЗ со стороны администраторов СДЗ.

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-3** и реализацией политики безопасности **Политика безопасности-2**, так как обеспечивает возможность управления параметрами СДЗ, влияющими на функции безопасности СДЗ.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-4** и реализацией политики безопасности **Политика безопасности-3,** так как обеспечивает доступ к информационным ресурсам в случае успешной проверки подлинности операционной системы с использованием ФБ СДЗ.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-4**, так как обеспечивает возможность проверки подлинности пользователей в соответствии с атрибутами безопасности и установленными ролями.

6.2.2. Обоснование целей безопасности для среды

В таблице 6.2 приведено отображение целей безопасности на предположения безопасности, угрозы и политику безопасности организации.

Таблица 6.2

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

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-6	Цель для среды функционирования ОО-7
Предположение-1	X						
Предположение-2		X					
Предположение-3			X				
Предположение-4					X		
Предположение-5						X	
Предположение-6							X
Угроза среды-1				X		X	
Угроза среды-2						X	

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1,** так как обеспечивается совместимость компонентов СДЗ с элементами информационной системы.

Цель для среды функционирования ОО-2

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-2**, так как обеспечивает установку, настройку и управление атрибутами безопасности в соответствии с эксплуатационной документацией.

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-1** и реализацией предположения безопасности **Предположение-3**, так как обеспечивается расположение СДЗ в пределах контура средств контроля доступа.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-1**, так как обеспечивает защиту области для выполнения функций безопасности СДЗ.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-4**, так как обеспечивает возможность поддержки средств аудита, используемых в ОО.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды **Угроза для среды-1, Угроза для среды-2** и реализацией предположения безопасности **Предположение-5**, так как обеспечивает условия безопасного функционирования и отсутствие в составе системного ПО и прикладного ПО средств для перезаписи (перепрограммирования) СДЗ и обеспечивает невозможность отключения (обхода) компонентов СДЗ.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо с реализацией предположения безопасности **Предположение-6,** так как, при руководстве эксплуатационной документацией, обеспечивается надлежащее функционирование ОО.

6.2. Обоснование требований безопасности

6.2.1. Обоснование требований безопасности для ОО

6.2.1.1. Обоснование функциональных требований безопасности ОО

В таблице 6.3 представлено отображение функциональных требований безопасности на цели безопасности для ОО.

Таблица 6.3

Отображение функциональных требований безопасности на цели безопасности

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4
FIA_AFL.1				**X**
FIA_UAU.1				**X**
FIA_UID.1				**X**
FMT_SMF.1	**X**	**X**	**X**	
FDP_ACC.1			**X**	
FDP_ACF.1			**X**	
FMT_MTD.1		**X**		
FMT_MSA.1		**X**	**X**	
FMT_MSA.3		**X**	**X**	**X**
FMT_SMR.1	**X**			

Включение указанных в таблице 6.3 функциональных требований безопасности ОО в ПЗ определяется проектом нормативного правового акта ФСТЭК России «Требования к средствам доверенной загрузки».

FDP_ACC.1 Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает реализацию политики ограниченного доступа для субъектов, именованных объектов и всех операций между субъектами и объектами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Выполнение требований данного компонента обеспечивает осуществление политики доступа, основываясь на атрибутах безопасности, определении правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает ограничение попыток пройти процедуру аутентификации для лиц, не являющихся уполномоченными пользователями или администраторами. При достижении определенного администратором СДЗ числа неуспешных попыток аутентификации некоторого лица, СДЗ предпринимаются действия, направленные на дальнейшее предотвращение попыток доступа со стороны данного лица, ограниченное временным интервалом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FIA_UAU.1 Выбор момента аутентификации

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа до того, как ФБО разрешат ему выполнять другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FIA_UID.1 Выбор момента идентификации

Выполнение требований данного компонента обеспечивает выполнение идентификации субъекта доступа до того, как ФБО разрешат ему выполнять другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FMT_SMF.1 Спецификация функций управления

Выполнение требований данного компонента обеспечивает наличие у ОО, как минимум, функций управления режимом выполнения функций безопасности и функций управления данными ФБО. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3** и способствует их достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность со стороны администраторов управлять данными (данными СДЗ), используемыми функциями безопасности СДЗ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента предоставляет возможность со стороны администраторов управлять атрибутами безопасности, используемыми функциями безопасности СДЗ. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2, Цель безопасности-2** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента предоставляет возможность

со стороны администраторов управлять атрибутами безопасности, используемыми функциями безопасности СДЗ. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2, Цель безопасности-3, Цель безопасности-4** и способствует их достижению.

FMT_SMR.1 Роли безопасности

Выполнение требований данного компонента обеспечивает поддержание ролей безопасности и их ассоциации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

6.2.1.2. Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ПЗ соответствуют ОУД2, усиленному компонентом ALC_FLR.1 «Базовое устранение недостатков» и расширенному компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства доверенной загрузки».

Включение указанных требований доверия к безопасности ОО в ПЗ определяется проектом нормативного правового акта ФСТЭК России «Требования к средствам доверенной загрузки».

6.2.2. Обоснование требований безопасности для среды ИТ

В таблице 6.4 представлено отображение функциональных требований безопасности среды ИТ на цели безопасности для среды.

Таблица 6.4

Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	Цель для среды функционирования ОО-4
FMT_SMR.1	**X**

FMT_SMR.1 Роли безопасности

Выполнение требований данного компонента обеспечивает выполнение поддержки ролей безопасности и осуществления ассоциаций пользователей с ролями в среде функционирования ОО. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО -4** и способствует ее достижению.

6.2.3. Обоснование удовлетворения зависимостей требований

В таблице 6.5 представлены результаты удовлетворения зависимостей функциональных требований. Все зависимости компонентов требований удовлетворены в настоящем профиле защиты либо включением компонентов, определенных в ГОСТ Р ИСО/МЭК 15408–2 под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в ГОСТ Р ИСО/МЭК 15408–2 под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 6.5 является справочным и содержит компоненты, определенные в ГОСТ Р ИСО/МЭК 15408–2 в описании компонентов требований, приведенных в столбце 1 таблицы 6.5, под рубрикой «Зависимости».

Столбец 3 таблицы 6.5 показывает, какие компоненты требований были включены в настоящий ПЗ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 6.5. Компоненты требований в столбце 3 таблицы 6.5 либо совпадают с компонентами в столбце 2 таблицы 6.5, либо иерархичны по отношению к ним.

Таблица 6.5

Зависимости функциональных требований

Функциональные компоненты	Зависимости по ГОСТ Р ИСО/МЭК 15408	Удовлетворение зависимостей
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	FDP_ACC.1 или FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1

Все зависимости включенных в ПЗ компонентов ФТБ удовлетворены.