ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России
30 декабря 2013 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ

ИТ.СДЗ.УБ4.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 СДЗ. 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 базовой системы ввода-вывода четвертого класса защиты.
Тип СДЗ:	СДЗ уровня базовой системы ввода-вывода.

Класс защиты:	Четвертый.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.СДЗ.УБ4.ПЗ.
Идентификация ОО:	СДЗ уровня базовой системы ввода-вывода.
Уровень доверия:	Оценочный уровень доверия 3 (ОУД3), усиленный компонентами ACM_CAP.4 «Поддержка генерации, процедуры приемки», ADV_IMP.2 «Реализация ФБО», ADV_LLD.1 «Описательный проект нижнего уровня», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VLA.3 «Умеренно стойкий», 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, ОУД3.

1.3. Аннотация профиля защиты

Настоящий ПЗ определяет требования безопасности для средств доверенной загрузки уровня базовой системы ввода-вывода (объекта оценки).

Объект оценки представляет собой программно-техническое средство, которое встраивается в базовую систему ввода-вывода и должно обеспечивать невозможность подключения нарушителя в разрыв между базовой системой ввода-вывода и средством доверенной загрузки для несанкционированного доступа.

Объект оценки должен обеспечивать нейтрализацию следующих угроз безопасности информации:

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;

отключение и (или) обход нарушителями компонентов средств доверенной загрузки;

несанкционированное изменение конфигурации (параметров) средства доверенной загрузки;

преодоление или обход функций безопасности средств доверенной загрузки.

В СДЗ уровня базовой системы ввода-вывода должны быть реализованы следующие функции безопасности:

разграничение доступа к управлению СДЗ;

управление работой СДЗ;

управление параметрами СДЗ;

аудит безопасности СДЗ;

тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ;

контроль компонентов СВТ;

блокирование загрузки операционной системы средством доверенной загрузки;

сигнализация средства доверенной загрузки;

обеспечение безопасности после завершения работы СДЗ.

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 доверенного канала при удаленном управлении СДЗ и взаимодействии с другими средствами защиты информации и доверенного маршрута при взаимодействии с уполномоченными субъектами;

обеспечение условий безопасного функционирования (расширенные возможности аудита безопасности), идентификации и аутентификации пользователей и администраторов СДЗ;

управление атрибутами безопасности компонентов средств доверенной загрузки;

защита от отключения (обхода).

В ПЗ изложены следующие виды требований безопасности, предъявляемые к СДЗ уровня базовой системы ввода-вывода:

функциональные требования безопасности;

требования доверия к безопасности.

Функциональные требования безопасности СДЗ, изложенные в ПЗ, включают:

требования к обеспечению блокирования СДЗ загрузки операционной системы в случае нарушения безопасности;

требования к действиям при попытке обхода СДЗ;

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 к аудиту функционирования СДЗ;

требования к тестированию СДЗ;

требования к контролю целостности программного обеспечения и параметров СДЗ;

требования к контролю компонентов аппаратного обеспечения СВТ.

Функциональные требования безопасности для СДЗ выражены на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408-2 и специальных компонентов.

Состав функциональных требований безопасности (ФТБ), включенных в настоящий ПЗ, обеспечивает следующие функциональные возможности СДЗ:

возможность регистрации возникновения событий, относящихся к безопасности и контролируемых средством доверенной загрузки;

возможность реагирования на обнаружение событий, указывающих на возможное нарушение безопасности;

возможность контроля целостности загружаемой операционной системы;

возможность со стороны администраторов СДЗ управлять режимом выполнения функций безопасности средства доверенной загрузки;

возможность со стороны администраторов СДЗ управлять данными (данными средства доверенной загрузки), 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;

возможность тестирования (самотестирования) функций безопасности средства доверенной загрузки, проверки целостности программного обеспечения средства доверенной загрузки и целостности данных средства доверенной загрузки;

блокирование загрузки операционной системы при выявлении попыток загрузки нештатной операционной системы;

блокирование загрузки операционной системы при превышении числа неудачных попыток аутентификации пользователя;

блокирование загрузки операционной системы при нарушении целостности средства доверенной загрузки;

блокирование загрузки операционной системы при нарушении целостности загружаемой программной среды;

блокирование загрузки операционной системы при критичных типах сбоев и ошибок.

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 3 (ОУД3), усиленный компонентами ACM_CAP.4 «Поддержка генерации, процедуры приемки», ADV_IMP.2 «Реализация ФБО», ADV_LLD.1 «Описательный проект нижнего уровня», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные

средства разработки», AVA_VLA.3 «Умеренно стойкий» 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, 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 базовой системы ввода-вывода.

Объект оценки представляет собой программно-техническое средство, которое встраивается в базовую систему ввода-вывода и осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, 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.

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 регистрации возникновения событий, относящихся к безопасности и контролируемых средством доверенной загрузки;

возможность реагирования на обнаружение событий, указывающих на возможное нарушение безопасности;

возможность контроля целостности загружаемой операционной системы;

возможность со стороны администраторов СДЗ управлять режимом выполнения функций безопасности средства доверенной загрузки;

возможность со стороны администраторов СДЗ 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;

возможность тестирования (самотестирования) функций безопасности средства доверенной загрузки, проверки целостности программного обеспечения средства доверенной загрузки и целостности данных средства доверенной загрузки;

блокирование загрузки операционной системы при выявлении попыток загрузки нештатной операционной системы;

блокирование загрузки операционной системы при превышении числа неудачных попыток аутентификации пользователя;

блокирование загрузки операционной системы при нарушении целостности средства доверенной загрузки;

блокирование загрузки операционной системы при нарушении целостности загружаемой программной среды;

блокирование загрузки операционной системы при критичных типах сбоев и ошибок.

СДЗ уровня базовой системы ввода-вывода встраиваются в базовую систему ввода-вывода и должны обеспечивать невозможность подключения нарушителя в разрыв между базовой системой ввода-вывода и СДЗ путем реализации следующих процессов:

получение управления в процессе выполнения базовой системы ввода-вывода до передачи управления для загрузки операционной системы с машинного носителя информации;

самотестирование средства доверенной загрузки;

идентификация и аутентификация пользователя с использованием портов ввода-вывода средства вычислительной техники;

контроль целостности среды функционирования (программной среды и элементов аппаратного обеспечения средства вычислительной техники);

продолжение выполнения базовой системы ввода-вывода с последующей загрузкой операционной системы в случае положительной аутентификации пользователя;

блокировка загрузки в случае превышения неудачных попыток аутентификации пользователя или попытки загрузки нештатной операционной системы;

регистрация событий безопасности и запись информации аудита в выделенную область памяти.

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

Должен быть обеспечен доверенный канал при удаленном управлении ОО и взаимодействии с другими средствами защиты информации и доверенный маршрут при взаимодействии с уполномоченными субъектами.

Предположение-4

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

Предположение-5

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

Предположение-6

Должна быть обеспечена ассоциация пользователей с соответствующими атрибутами безопасности (идентификаторы, группы, роли и др.)

Предположение-7

Должна быть обеспечена синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования.

Предположение-8

Должна быть обеспечена невозможность отключения (обхода) компонентов ОО.

Предположение, имеющее отношение к персоналу

Предположение-9

Персонал, ответственный за функционирование ОО, должен обеспечивать надлежащее функционирование ОО, руководствуясь эксплуатационной документацией.

3.2. Угрозы безопасности информации

3.2.1. Угрозы, которым должен противостоять объект оценки

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 блокирования загрузки нештатной 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-2

1. Аннотация угрозы – нарушение целостности программной среды средств СВТ и (или) состава компонентов аппаратного обеспечения СВТ в ИС.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированное изменение программной среды СВТ и (или) извлечение (подмена), модификация компонентов аппаратного обеспечения СВТ.

4. Используемые уязвимости – недостатки, связанные с возможностью осуществления доступа к оборудованию, отсутствие механизмов контроля целостности программной среды и состава компонентов СВТ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – программная среда СВТ, аппаратные компоненты СВТ.

6. Нарушаемые свойства безопасности информационных ресурсов – целостность, 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 – обход нарушителями компонентов СДЗ.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

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

4. Используемые уязвимости – недостатки механизмов управления доступом, физической защиты оборудования ИС.

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

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

7. Возможные последствия реализации угрозы – нарушение режимов функционирования СДЗ; доступность ресурсов ИС, СДЗ.

Угроза-4

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, физической защиты оборудования в ИС.

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.

3.2.2. Угрозы, которым должна противостоять среда

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

Угроза среды-1

1. Аннотация угрозы – отключение (обход) или блокирование базовой системы ввода-вывода.

2. Источники угрозы – внутренний нарушитель.

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

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 – преодоление или обход идентификации/аутентификации за счет недостаточного качества аутентификационной информации.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – преодоление или обход идентификации/аутентификации.

4. Используемая уязвимость – недостатки механизмов идентификации/аутентификации.

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

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

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

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

Должно осуществляться управление со стороны администраторов СДЗ режимами выполнения функций безопасности СДЗ.

Политика безопасности-3

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

Политика безопасности-4

Объект оценки должен осуществлять механизмы идентификации и аутентификации (распознавание, проверку подлинности и полномочий уполномоченных пользователей и администраторов).

Политика безопасности-5

Должна быть обеспечена невозможность несанкционированной загрузки ОС с нештатных носителей. Также объект оценки должен быть защищен от несанкционированного доступа и нарушений в отношении функций безопасности ОО.

Политика безопасности-6

Должны быть обеспечены надлежащие механизмы регистрации и предупреждения (сигнализации) о любых событиях, относящихся к возможным нарушениям безопасности.

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 работой СДЗ

Объект оценки должен обеспечивать управление со стороны администраторов СДЗ режимами выполнения функций безопасности СДЗ.

Цель безопасности-3

Управление параметрами СДЗ

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

Цель безопасности-4

Тестирование и контроль целостности

Объект оценки должен осуществлять обеспечение контроля целостности параметров СДЗ и загружаемой операционной системы. Должно осуществляться выполнение встроенных в СДЗ тестов, направленных на проверку корректности работы механизмов СДЗ.

Цель безопасности-5

Блокирование СДЗ

Функции безопасности объекта оценки должны осуществлять блокировку загрузки ОС при выявлении попыток обхода механизмов защиты.

Цель безопасности-6

Аудит безопасности СДЗ

Объект оценки должен располагать надлежащими механизмами регистрации и предупреждения (сигнализации) администратора о любых событиях, относящихся к возможным нарушениям 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

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

Цель для среды функционирования ОО-4

Поддержка аудита

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

Цель для среды функционирования ОО-5

Защита данных ФБО

Должна быть обеспечена защищенная область для выполнения функций безопасности СДЗ.

Цель для среды функционирования ОО-6

Управление атрибутами безопасности

Должна быть обеспечена ассоциация пользователей с соответствующими атрибутами безопасности (идентификаторы, группы, роли и др.), а также возможность управления атрибутами безопасности компонентов СДЗ в СВТ (ИС) только уполномоченными администраторами в соответствии с отведенными им ролями.

Цель для среды функционирования ОО-7

Обеспечение условий безопасного функционирования

Отсутствие в среде функционирования СДЗ в составе системного ПО, прикладного и специального ПО средств (специализированных инструментальных средств) для перезаписи (перепрограммирования) СДЗ. Обеспечение невозможности отключения (обхода) компонентов СДЗ.

Цель для среды функционирования ОО-8

Синхронизация по времени

Должен быть обеспечен надлежащий источник меток времени и синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования.

Цель для среды функционирования ОО-9

Требования к персоналу

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

Цель для среды функционирования ОО-10

Доверенный канал и маршрут

Должен быть обеспечен доверенный канал при удаленном управлении ОО и взаимодействии с другими средствами защиты информации и доверенного маршрута при взаимодействии с уполномоченными субъектами.

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. Кроме того, в настоящий ПЗ включен ряд требований безопасности, сформулированных в явном виде (расширение 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 ОУД3, усиленного компонентами ACM_CAP.4 «Поддержка генерации, процедуры приемки», ADV_IMP.2 «Реализация ФБО», ADV_LLD.1 «Описательный проект нижнего уровня», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VLA.3 «Умеренно стойкий» 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

Идентификатор компонента требований	Название компонента требований
FAU_ARP.1	Сигналы нарушения безопасности
FAU_GEN.1	Генерация данных аудита
FDP_SDI.1	Целостность хранимых данных
FMT_SMF.1	Спецификация функций управления
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MTD.1	Управление данными функций безопасности
FMT_MTD.2	Управление ограничениями данных функций безопасности
FMT_SMR.1	Роли безопасности
FPT_TST.1	Тестирование ФБО
FTL_BLC_EXT.1	Блокировка загрузки операционной системы

5.1.1.1. Аудит безопасности (FAU)

FAU_ARP.1 Сигналы нарушения безопасности

FAU_ARP.1.1 ФБО должны предпринять [информирование администратора СДЗ, [назначение: *список других действий*]] при обнаружении возможного нарушения безопасности.

Зависимости: FAU_SAA.1 «Анализ потенциального нарушения».

Замечания по применению: Разработчик ЗБ, кроме информирования администратора СДЗ, может перечислить и другие действия при обнаружении возможного нарушения безопасности (попытка загрузки нештатной операционной системы, обнаружение нарушения целостности ПО СДЗ или среды функционирования и др.). В этом случае разработчику ЗБ необходимо будет четко определить последовательность проведения таких действий.

FAU_GEN.1 Генерация данных аудита

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

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на [выбор: *минимальный, базовый, детализированный, неопределенный*] уровне аудита;

в) [назначение: *другие специально определенные события, потенциально подвергаемые аудиту*].

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

а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ/ЗБ, [назначение: *другая относящаяся к аудиту информация*].

Зависимости: FPT_STM.1 «Надежные метки времени».

Замечания по применению: В пункте б) FAU_GEN.1.1 разработчик ЗБ может выбрать уровень аудита минимальный, базовый или детализированный и следовать инструкциям ГОСТ Р ИСО/МЭК 15408-2 по включению в FAU_GEN.1 событий согласно соответствующему выбранному уровню аудита пункту в рубрике «Аудит» для каждого функционального компонента из ГОСТ Р ИСО/МЭК 15408-2, включенного в ПЗ/ЗБ. Если в пункте б) FAU_GEN.1.1 разработчик ЗБ определит уровень аудита как неопределенный, то от него потребуется самостоятельно для каждого функционального компонента из ГОСТ Р ИСО/МЭК 15408-2 и специального компонента ФТБ, включенного в ПЗ/ЗБ, определить события, потенциально подвергаемые аудиту (неуспешная идентификация/аутентификация пользователя, попытка загрузки нештатной операционной системы, обнаружение нарушения целостности ПО СДЗ или среды функционирования и (или) др.).

5.1.1.2. Защита данных пользователя (FDP)

FDP_SDI.1 Мониторинг целостности хранимых данных

FDP_SDI.1.**1** ФБО должны контролировать **[назначение: программная среда] объекты загружаемой операционной системы и [назначение: другие виды контролируемой информации], хранимые** в пределах области действия функции безопасности, на наличие [назначение: *ошибки целостности*], основываясь на следующих атрибутах: [назначение: *атрибуты **контролируемых** данных*].

Зависимости: отсутствуют.

Замечания по применению: По отношению к СДЗ принято допустимым рассматривать загружаемую операционную систему в качестве данных пользователя.

В качестве объектов загружаемой операционной системы могут рассматриваться исполняемые файлы и файлы данных операционной системы, параметры настройки операционной системы.

В качестве других видов контролируемой информации могут рассматриваться исполняемые файлы и параметры настройки средств защиты информации, применяемые на средстве вычислительной техники.

В качестве атрибутов контролируемых данных могут рассматриваться уникальная идентификация, контрольная сумма и др.

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, [назначение: *список других функций управления безопасностью, предоставляемых ФБО*].

Зависимости: отсутствуют.

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны ограничить возможность [выбор: *определения режима выполнения, отключения, подключения, модификации режима выполнения*] определенных функций [назначение: *список функций*] только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 «Роли безопасности»,
FMT_SMF.1 «Спецификация функций управления».

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_MTD.2 Управление ограничениями данных ФБО

FMT_MTD.2.1 ФБО должны предоставить возможность определения ограничений следующих данных [назначение: *список данных ФБО*] только [назначение: *уполномоченные идентифицированные роли*].

FMT_MTD.2.2 ФБО должны предпринять следующие действия при достижении или превышении данными ФБО установленных выше ограничений **[**назначение: *предпринимаемые действия*]**.**

Зависимости: FMT_MTD.1 «Управление данными ФБО»,
FMT_SMR.1 «Роли безопасности».

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.

5.1.1.4. Защита ФБО (FPT)

FPT_TST.1Тестирование ФБО

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования [выбор: *при запуске, периодически в процессе нормального функционирования, по запросу уполномоченного пользователя, при условиях [назначение: условия, при которых следует предусмотреть самотестирование]*] для демонстрации правильного выполнения ФБО.

FPT_TST.1.2 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО.

FPT_TST.1.3 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность хранимого выполняемого кода ФБО.

Зависимости: FPT_AMT.1 «Тестирование абстрактной машины».

5.1.1.5. Безопасность доверенной загрузки (FTL)

FTL_BLC_EXT.1 Блокировка загрузки операционной системы

FTL_BLC_EXT.1.1 ФБО должны обеспечивать блокирование загрузки операционной системы при выявлении попыток загрузки нештатной операционной системы.

FTL_BLC_EXT.1.2 ФБО должны обеспечивать блокирование загрузки операционной системы при превышении числа неудачных попыток аутентификации пользователя.

FTL_BLC_EXT.1.3 ФБО должны обеспечивать блокирование загрузки операционной системы при нарушении целостности средства доверенной загрузки.

FTL_BLC_EXT.1.4 ФБО должны обеспечивать блокирование загрузки операционной системы при нарушении *целостности загружаемой программной среды*.

FTL_BLC_EXT.1.5 ФБО должны обеспечивать блокирование загрузки операционной системы при критичных типах сбоев и ошибок.

Зависимости: FDP_SDI.1 «Целостность хранимых данных» или FTL_SVT.1 «Контроль компонентов аппаратного обеспечения средства вычислительной техники».

Замечания по применению: В качестве критичных типов сбоев и ошибок следует рассматривать такие ошибки или сбои, для которых требуется аварийная поддержка и восстановление, которые затрагивают функции безопасности и не могут быть устранены, например, путем повторного запуска.

5.1.2. Требования доверия к безопасности объекта оценки

Требования доверия к безопасности ОО взяты из ГОСТ Р ИСО/МЭК 15408–3 и образуют ОУД3, усиленный компонентами ACM_CAP.4 «Поддержка генерации, процедуры приемки», ADV_IMP.2 «Реализация ФБО», ADV_LLD.1 «Описательный проект нижнего уровня», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VLA.3 «Умеренно стойкий» 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.4	Поддержка генерации, процедуры приемки
	ACM_SCP.1	Охват управления конфигурацией (УК) объекта оценки
Поставка и эксплуатация	ADO_DEL.1	Процедуры поставки
	ADO_IGS.1	Процедуры установки, генерации и запуска

Окончание таблицы 5.2

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Разработка	ADV_FSP. 1	Неформальная функциональная спецификация
	ADV_HLD.2	Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.2*	Реализация ФБО
	ADV_LLD.1	Описательный проект нижнего уровня
	ADV_RCR.1*	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Поддержка жизненного цикла	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR.1	Базовое устранение недостатков
	ALC_TAT.1	Полностью определенные инструментальные средства разработки
Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.1	Тестирование: проект верхнего уровня
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_MSU.1	Экспертиза руководств
	AVA_SOF.1	Оценка стойкости функции безопасности ОО
	AVA_VLA.3	Умеренно стойкий
Обновление СДЗ	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность средства доверенной загрузки
* – Отмечены компоненты, конкретизированные в настоящем ПЗ для обеспечения преемственности требованиям по контролю отсутствия недекларированных возможностей, изложенных в Руководящем документе ФСТЭК (Гостехкомиссии) России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации: Классификация по уровню контроля отсутствия недекларированных возможностей», 1999.		

5.1.2.1. Управление конфигурацией (ACM)

ACM_CAP.4 Поддержка генерации, процедуры приемки

Зависимости

ACM_SCP.1 Охват УК объекта оценки,

ALC_DVS.1 Идентификация мер безопасности.

Элементы действий разработчика

ACM_CAP.4.1D Разработчик должен предоставить маркировку для ОО.

ACM_CAP.4.2D Разработчик должен использовать систему УК.

ACM_CAP.4.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_CAP.4.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.4.2C ОО должен быть помечен маркировкой.

ACM_CAP.4.3C Документация УК должна включать в себя список конфигурации, план УК и план приемки.

ACM_CAP.4.4C Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

ACM_CAP.4.5C Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

ACM_CAP.4.6C Система УК должна уникально идентифицировать все элементы конфигурации.

ACM_CAP.4.7C План УК должен содержать описание, как используется система УК.

ACM_CAP.4.8C Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

ACM_CAP.4.9C Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

ACM_CAP.4.10C Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

ACM_CAP.4.11C Система УК должна поддерживать генерацию ОО.

ACM_CAP.4.12C План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части ОО.

Элементы действий оценщика

ACM_CAP.4.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ACM_SCP.1 Охват УК объекта оценки

Зависимости

ACM_CAP.3 Средства контроля авторизации.

Элементы действий разработчика

ACM_SCP.1.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_SCP.1.1C Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора и документацию УК.

ACM_SCP.1.2C Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

Элементы действий оценщика

ACM_SCP.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_DEL.1 Процедуры поставки

Зависимости отсутствуют.

Элементы действий разработчика

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

ADO_DEL.1.2 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 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

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 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.2 Детализация вопросов безопасности в проекте верхнего уровня

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ADV_RCR.1 Неформальная демонстрация соответствия.

Элементы действий разработчика

ADV_HLD.2.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.2.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.2.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.2.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.2.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.2.5C 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.2.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.2.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.2.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.2.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

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_IMP.2 Реализация ФБО

Зависимости

ADV_LLD.1 Описательный проект нижнего уровня,

ADV_RCR.1 Неформальная демонстрация соответствия,

ALC_TAT.1 Полностью определенные инструментальные средства разработки.

Элементы действий разработчика

ADV_IMP.2.1D Разработчик должен обеспечить представление реализации для всех ФБО **на уровне исходных текстов всего программного обеспечения, входящего в состав ОО, а также указать в документации значения контрольных сумм файлов, входящих в состав ОО**.

Элементы содержания и представления свидетельств

ADV_IMP.2.1C Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

ADV_IMP.2.2C Представление реализации должно быть внутренне непротиворечивым.

ADV_IMP.2.3C Представление реализации должно включать в себя описание взаимосвязей между всеми частями реализации.

Элементы действий оценщика

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

ADV_IMP.2.2E Оценщик должен сделать независимое заключение, что представление реализации – точное и полное отображение функциональных требований безопасности ОО, **в том числе на основе результатов:**

контроля исходного состояния ПО;

контроля полноты и отсутствия избыточности исходных текстов на уровне файлов.

ADV_LLD.1 Описательный проект нижнего уровня

Зависимости

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня,

ADV_RCR.1 Неформальная демонстрация соответствия.

Элементы действий разработчика

ADV_LLD.1.1D Разработчик должен представить проект нижнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_LLD.1.1C Представление проекта нижнего уровня должно быть неформальным.

ADV_LLD.1.2C Проект нижнего уровня должен быть внутренне непротиворечивым.

ADV_LLD.1.3C Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

ADV_LLD.1.4C Проект нижнего уровня должен содержать описание назначения каждого модуля.

ADV_LLD.1.5C Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

ADV_LLD.1.6C Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

ADV_LLD.1.7C Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

ADV_LLD.1.8C Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

ADV_LLD.1.9C Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_LLD.1.10C Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

Элементы действий оценщика

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

ADV_LLD.1.2E Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 (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.

ADV_RCR.1 (2) Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_RCR.1.1D Разработчик должен представить анализ соответствия между **исходными текстами программного обеспечения и его объектным (загрузочным) кодом**.

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для **смежной пары представлений ФБО, указанных в ADV_RCR.1.1D,** 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. Поддержка жизненного цикла (ALC)

ALC_DVS.1 Идентификация мер безопасности

Зависимости отсутствуют.

Элементы действий разработчика

ALC_DVS.1.1D Разработчик должен иметь документацию по безопасности разработки.

Элементы содержания и представления свидетельств

ALC_DVS.1.1C Документация по безопасности разработки должна содержать описание всех физических, процедурных, относящихся к персоналу и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.

ALC_DVS.1.2C Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

Элементы действий оценщика

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

ALC_DVS.1.2E Оценщик должен подтвердить применение мер безопасности.

ALC_FLR.1 Базовое устранение недостатков

Зависимости отсутствуют.

Элементы действий разработчика

ALC_FLR.11D Разработчик должен задокументировать процедуры устранения недостатков.

Элементы содержания и представления свидетельств

ALC_FLR.1.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждой редакции ОО.

ALC_FLR.1.2C Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.

ALC_FLR.1.3C Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

ALC_FLR.1.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Элементы действий оценщика

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

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Зависимости

ADV_IMP.1 Подмножество реализации ФБО.

Элементы действий разработчика

ALC_TAT.1.1D Разработчик должен идентифицировать инструментальные средства разработки ОО.

ALC_TAT.1.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.

Элементы содержания и представления свидетельств

ALC_TAT.1.1C Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

ALC_TAT.1.2C Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

ALC_TAT.1.3C Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.

Элементы действий оценщика

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

5.1.2.6. Тестирование (ATE)

ATE_COV.2 Анализ покрытия

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ATE_FUN.1 Функциональное тестирование.

Элементы действий разработчика

ATE_COV.2.1D Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

ATE_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой

документации, и описанием ФБО в функциональной спецификации.

ATE_COV.2.2C Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

Элементы действий оценщика

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

ATE_DPT.1 Тестирование: проект верхнего уровня

Зависимости

ADV_HLD.1 Описательный проект верхнего уровня,

ATE_FUN.1 Функциональное тестирование.

Элементы действий разработчика

ATE_DPT.1.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.1.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.

Элементы действий оценщика

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

ATE_FUN.1 Функциональное тестирование

Зависимости отсутствуют.

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

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

AGD_ADM.1 Руководство администратора,

AGD_USR.1 Руководство пользователя,

ATE_FUN.1 Функциональное 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.

5.1.2.7. Оценка уязвимостей (AVA)

AVA_MSU.1 Экспертиза руководств

Зависимости

ADO_IGS.1 Процедуры установки, генерации и запуска,

ADV_FSP.1 Неформальная функциональная спецификация,

AGD_ADM.1 Руководство администратора,

AGD_USR.1 Руководство пользователя.

Элементы действий разработчика

AVA_MSU.1.1D Разработчик должен представить руководства по применению ОО.

Элементы содержания и представления свидетельств

AVA_MSU.1.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.1.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.1.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.1.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

Элементы действий оценщика

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

AVA_MSU.1.2E Оценщик должен повторить все процедуры конфигурирования и установки для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.1.3E Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

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 ЗБ как имеющего утверждение относительно стойкости функции безопасности ОО.

Элементы содержания и представления свидетельств

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

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

Элементы действий оценщика

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

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

AVA_VLA.3 Умеренно стойкий

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня,

ADV_IMP.1 Подмножество реализации ФБО,

ADV_LLD.1 Описательный проект нижнего уровня,

AGD_ADM.1 Руководство администратора,

AGD_USR.1 Руководство пользователя.

Элементы действий разработчика

AVA_VLA.3.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску путей, которыми пользователь может нарушить ПБО.

AVA_VLA.3.2D Разработчик должен задокументировать местоположение идентифицированных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.3.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.3.2C Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.

AVA_VLA.3.3C Свидетельство должно показать, что поиск уязвимостей является систематическим.

Элементы действий оценщика

AVA_VLA.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VLA.3.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.

AVA_VLA.3.3E Оценщик должен выполнить независимый анализ уязвимостей.

AVA_VLA.3.4E Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

AVA_VLA.3.5E Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим умеренным потенциалом нападения.

5.1.2.8. 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
FAU_SAA.1	Анализ потенциального нарушения
FIA_UAU.1	Выбор момента аутентификации
FIA_UID.1	Выбор момента идентификации
FPT_AMT.1	Анализ потенциального нарушения
FPT_STM.1	Надежные метки времени

5.2.1. Аудит безопасности (FAU)

FAU_SAA.1 Анализ потенциального нарушения

FAU_SAA.1.1 ФБ среды функционирования должны быть способны применить набор правил мониторинга событий, подвергающихся аудиту, и указать на возможное нарушение ПБО, основываясь на этих правилах.

FAU_SAA.1.2 ФБ среды функционирования должны реализовать следующие правила при мониторинге событий, подвергающихся аудиту:

а) накопление или объединение известных [назначение: *подмножество определенных событий, потенциально подвергаемых аудиту*], указывающих на возможное нарушение безопасности;

б) [назначение: *другие правила*].

Зависимости: FAU_GEN.1 Генерация данных аудита.

5.2.2. Идентификация и аутентификация (FIA)

FIA_UAU.1 Выбор момента аутентификации

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

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

Зависимости отсутствуют.

5.2.3. Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 ФБ среды функционирования должны выполнять пакет тестовых программ [выбор: *при первоначальном запуске, периодически во время нормального функционирования, по запросу администратора безопасности, при других условиях*] для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу ФБО.

Зависимости отсутствуют.

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	Цель безопасности-5	Цель безопасности-6
Угроза-1		X	X		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		
Политика безопасности-5					X	
Политика безопасности-6						X

Цель безопасности-1

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

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-1** и реализацией политики безопасности **Политика безопасности-2**, так как обеспечивает возможность управления режимами выполнения функций безопасности СДЗ.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-4** и реализацией политики безопасности **Политика безопасности-3**, так как обеспечивает возможность управления параметрами СДЗ, влияющими на функции безопасности СДЗ.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-4**, так как обеспечивает контроль целостности параметров СДЗ, а также обеспечивает проверку корректности работы механизмов СДЗ.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-3** и реализацией политики безопасности **Политика безопасности-5**, так как осуществляет блокировку загрузки ОС при обнаружении попыток обхода механизмов защиты.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-6,** так как обеспечивает возможность регистрации, предупреждения (сигнализации) и учета любых событий, относящихся к возможным нарушениям.

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	Цель для среды функционирования ОО-8	Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-10
Предположение-1	X									
Предположение-2		X								
Предположение-3										X
Предположение-4			X							
Предположение-5				X						
Предположение-6						X				
Предположение-7								X		
Предположение-8							X			
Предположение-9									X	
Угроза среды-1			X		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 обеспечивает 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-4**, так как обеспечивает невозможность осуществления действий, направленных на нарушение физической целостности компонентов СВТ, доступ к которым контролируется с применением СДЗ.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-5**, так как обеспечивает возможность поддержки средств аудита, используемых в ОО.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-1,** так как обеспечивает защищенную область в среде функционирования для выполнения ФБ СДЗ.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-2** и реализацией предположения безопасности **Предположение-6**, так как обеспечивает ассоциацию пользователей с соответствующими атрибутами безопасности и обеспечивает управление атрибутами безопасности СДЗ и объектов ИС только уполномоченным администраторам.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-1** и реализацией предположения безопасности **Предположение-8**, 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-8

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-7,** так как обеспечивается синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования.

Цель для среды функционирования ОО-9

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-9,** так как, руководствуясь эксплуатационной документацией, обеспечивается надлежащее функционирование ОО.

Цель для среды функционирования ОО-10

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-3,** так как обеспечивается доверенный канал и маршрут при удаленном управлении ОО и взаимодействии с другими средствами защиты информации.

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	Цель безопасности-5	Цель безопасности-6
FAU_ARP.1						**X**
FAU_GEN.1						**X**
FIA_AFL.1						
FIA_SOS.1						
FIA_UAU.2						
FIA_UID.2						
FDP_SDI.1				**X**		
FMT_SMF.1	**X**	**X**	**X**			
FMT_MOF.1	**X**	**X**				
FMT_MTD.1	**X**		**X**			
FMT_MTD.2	**X**		**X**			
FMT_SMR.1	**X**					
FPT_TST.1				**X**		
FTL_BLC_EXT.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».

FAU_ARP.1 Сигналы нарушения безопасности

Выполнение требований данного компонента способствует обнаружению попыток нарушения безопасности и обеспечивает функцию оповещения об этом администратора безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_GEN.1 Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита, и события, которые должны подвергаться аудиту. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FDP_SDI.1 Целостность хранимых данных

Выполнение требований данного компонента обеспечивает возможность контроля целостности загружаемой операционной системы. 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_MOF.1 Управление режимом выполнения функций безопасности

При выполнении требований данного компонента ФБО разрешает модификацию режима выполнения функций, связанных со сбором данных об ИС, их анализом и ответными реакциями, только администраторам СДЗ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

Выполнение требований данного компонента также обеспечивает возможность со стороны администраторов управлять работой (режимами СДЗ), используемыми функциями безопасности средства доверенной загрузки. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее 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 целями **Цель безопасности-1, Цель безопасности-3** и способствует их достижению.

FMT_MTD.2 Управление ограничениями данных ФБО

Выполнение требований данного компонента предоставляет возможность определения ограничений данных ФБО только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1**, **Цель безопасности-3** 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.

FPT_TST.1 Тестирование ФБО

Выполнение требований данного компонента обеспечивает возможность тестирования (самотестирования) функций безопасности СДЗ, проверки целостности программного обеспечения СДЗ и целостности данных СДЗ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FTL_BLC_EXT.1 Блокировка загрузки операционной системы

Выполнение требований данного компонента обеспечивает блокирование загрузки операционной системы при выявлении попыток загрузки нештатной операционной системы, при превышении числа неудачных попыток аутентификации пользователя, при нарушении целостности СДЗ, при нарушении целостности загружаемой программной среды (операционной системы), при критичных типах сбоев и ошибок. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

6.2.1.2. Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ПЗ соответствуют ОУДЗ, усиленного компонентами ACM_CAP.4 «Поддержка генерации, процедуры приемки», ADV_IMP.2 «Реализация ФБО», ADV_LLD.1 «Описательный проект нижнего уровня», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VLA.3 «Умеренно стойкий» 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	**Цель для среды функционирования ОО-5**
FAU_SAA.1		**X**
FIA_UAU.1		**X**
FIA_UID.1		**X**
FPT_AMT.1	**X**	
FPT_STM.1	**X**	

FAU_SAA.1 Анализ потенциального нарушения

Данный компонент включен в ПЗ, чтобы учесть зависимости выполнения требований компонента FAU_ARP.1. Выполнение требований данного компонента обеспечивает определение совокупности событий, потенциально подвергаемых аудиту, появление которых (каждого отдельно или в совокупности) указывает на потенциальные нарушения. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FIA_UAU.1 Выбор момента аутентификации

Данный компонент включен в ПЗ, чтобы учесть зависимости выполнения требований компонента FIA_AFL.1. Выполнение требований данного компонента обеспечивает ограничение попыток пройти процедуру аутентификации для лиц, не являющихся уполномоченными пользователями ОО. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FIA_UID.1 Выбор момента идентификации

Данный компонент включен в ПЗ, чтобы учесть зависимости выполнения требований компонента FIA_UAU.2. Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FPT_AMT.1 Тестирование абстрактной машины

Данный компонент включен в ПЗ, чтобы учесть зависимости выполнения требований компонента FPT_TST.1. Выполнение требований данного компонента обеспечивает тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной, перед использованием компонентов ОО. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-4** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ПЗ, для того, чтобы учесть зависимости выполнения требований компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени. 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
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1 для среды
FAU_GEN.1	FPT_STM.1	FPT_STM.1 для среды
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.2	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1 для среды
FPT_TST.1	FPT_AMT.1	FPT_AMT.1 для среды
FTL_BLC_EXT.1	FDP_SDI.1 FTL_SVT.1	FDP_SDI.1 FTL_SVT.1

Все зависимости включенных в ПЗ компонентов ФТБ удовлетворены.

_____