

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
1 декабря 2014 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**ПРОФИЛЬ ЗАЩИТЫ
СРЕДСТВ КОНТРОЛЯ ПОДКЛЮЧЕНИЯ СЪЕМНЫХ МАШИННЫХ
НОСИТЕЛЕЙ ИНФОРМАЦИИ
ШЕСТОГО КЛАССА ЗАЩИТЫ**

ИТ.СКН.П6.ПЗ

МОСКВА
2014

Содержание

1.	Общие положения	4
2.	Введение профиля защиты	5
2.1.	Ссылка на профиль защиты	5
2.2.	Аннотация объекта оценки	5
2.3.	Соглашения.....	9
3.	Утверждение соответствия.....	10
3.1.	Утверждение о соответствии ИСО/МЭК 15408.....	10
3.2.	Утверждение о соответствии профилям защиты.....	10
3.3.	Обоснование соответствия.....	10
3.4.	Изложение соответствия	10
4.	Цели безопасности	11
4.1.	Цели безопасности для среды функционирования.....	11
5.	Определение расширенных компонентов.....	13
5.1.	Определение расширенных компонентов функциональных требований безопасности.....	13
5.2.	Определение расширенных компонентов требований доверия к безопасности.....	15
6.	Требования безопасности	16
6.1.	Требования безопасности для объекта оценки	16
6.2.	Требования доверия к безопасности.....	19

Перечень сокращений

ЗБ	– задание по безопасности
ИС	– информационная система
ИТ	– информационная технология
ИФБО	– интерфейс функциональной возможности безопасности объекта оценки
ОО	– объект оценки
ОУД	– оценочный уровень доверия
ПБОр	– политика безопасности организации
ПЗ	– профиль защиты
ПО	– программное обеспечение
СВТ	– средство вычислительной техники
СКН	– средство контроля съемных машинных носителей информации
ТДБ	– требование доверия к безопасности
УК	– управление конфигурацией
ФБО	– функциональные возможности 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, 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 при проведении ими работ по сертификации средств контроля съемных машинных носителей информации (СКН) на соответствие Требованиям к средствам контроля съемных машинных носителей информации, утвержденным приказом ФСТЭК России от 28 июля 2014 г. № 87.

Для цели настоящего документа в качестве типов съемных машинных носителей информации рассматриваются флэш-накопители, внешние накопители на жестких дисках и иные устройства.

Настоящий методический документ ФСТЭК России детализирует и определяет взаимосвязи требований к функциям безопасности СКН, установленным Требованиями к средствам контроля съемных машинных носителей информации, утвержденными приказом ФСТЭК России от 28 июля 2014 г. № 87.

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».

2. Введение профиля защиты

Данный раздел содержит информацию общего характера. Подраздел «Ссылка на профиль защиты» включает идентификационные материалы профиля защиты, которые предоставляют маркировку и описательную информацию, необходимую, чтобы контролировать и идентифицировать профиль защиты (ПЗ) и объект оценки (ОО), к которому он относится. Подраздел «Аннотация объекта оценки» содержит краткое описание использования объекта оценки и его основные характеристики безопасности.

2.1. Ссылка на профиль защиты

Наименование ПЗ:	Профиль защиты средств контроля подключения съемных машинных носителей информации шестого класса защиты.
Тип СКН:	Средство контроля подключения съемных машинных носителей информации.
Класс защиты:	Шестой.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.СКН.П6.ПЗ.
Идентификация ОО:	Средство контроля подключения съемных машинных носителей информации.
Уровень доверия:	Оценочный уровень доверия 1 (ОУД1), расширенный компонентом АМА_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации».
Идентификация:	Требования к средствам контроля съемных машинных носителей информации, утвержденные приказом ФСТЭК России от 28 июля 2014 г. № 87. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
Ключевые слова:	Средства контроля съемных машинных носителей информации, контроль подключения съемных машинных носителей, ОУД1.

2.2. Аннотация объекта оценки

Настоящий ПЗ определяет требования безопасности для средств контроля подключения съемных машинных носителей информации (объекта оценки).

2.2.1. Использование и основные характеристики безопасности объекта оценки

Объект оценки представляет собой программное или программно-техническое средство, которое предназначено для обеспечения контроля использования интерфейсов ввода (вывода) средств вычислительной техники при подключении съемных машинных носителей информации.

Объект оценки должен обеспечивать нейтрализацию угроз безопасности информации, связанных с подключением к информационной системе внутренними и внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из информационной системы или загрузкой в информационную систему с этих съемных машинных носителей информации вредоносного программного обеспечения.

В состав средства контроля подключения съемных машинных носителей информации входят следующие компоненты:

- программное обеспечение, устанавливаемое на средствах вычислительной техники и обеспечивающее взаимодействие с подключаемыми съемными машинными носителями информации;

- программное обеспечение управления (локального и (или) централизованного) средствами контроля подключения съемных машинных носителей информации.

В СКН должны быть реализованы следующие функции безопасности:

- разграничение доступа к управлению СКН;

- управление работой СКН;

- контроль подключения съемных машинных носителей информации;

- аудит безопасности СКН.

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

- физическая защита средств вычислительной техники, на которых используются компоненты СКН;

- обеспечение условий безопасного функционирования СКН;

- управление атрибутами безопасности компонентов СКН.

Функции безопасности СКН должны обладать составом функциональных возможностей (функциональных требований безопасности), обеспечивающих реализацию этих функций.

В ПЗ изложены следующие виды требований безопасности, предъявляемые к средствам контроля подключения съемных машинных носителей информации:

- функциональные требования безопасности;

- требования доверия к безопасности.

Функциональные требования безопасности СКН, изложенные в ПЗ, включают:

- требования к разграничению доступа к управлению СКН;

требования к управлению параметрами СКН, которые влияют на выполнение функций безопасности СКН;

требования к контролю подключения съемных машинных носителей информации;

требования к аудиту безопасности СКН.

Функциональные требования безопасности для СКН выражены на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408–2 и специальных (расширенных) компонентов.

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

реализацию политики управления использованием подключаемых съемных машинных носителей информации по отношению к подключаемым произвольным съемным машинным носителям информации;

возможность управления использованием подключаемых произвольных съемных машинных носителей информации на основе анализа разрешений на подключение к конкретным интерфейсам ввода (вывода) средств вычислительной техники;

возможность со стороны администраторов СКН управлять данными (данными средства контроля подключения съемных машинных носителей информации), используемыми функциями безопасности средства контроля съемных машинных носителей информации;

поддержку определенных ролей для средства контроля подключения съемных машинных носителей информации и их ассоциации с конкретными администраторами СКН и пользователями информационной системы;

возможность регистрации событий, связанных с изменениями конфигурации функций безопасности средства контроля подключения съемных машинных носителей информации;

возможность читать информацию из записей аудита уполномоченным администраторам СКН.

Требования доверия к безопасности средств контроля подключения съемных машинных носителей информации сформированы на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408–3 и специальных (расширенных) компонентов.

Требования доверия к безопасности средствам контроля подключения съемных машинных носителей информации образуют оценочный уровень доверия 1 (ОУД1), расширенный компонентом АМА_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации».

В целях обеспечения условий для безопасного функционирования СКН в настоящем ПЗ определены цели для среды функционирования СКН.

2.2.2. Тип объекта оценки

Объектом оценки в настоящем ПЗ является средство контроля подключения съемных машинных носителей информации.

Объект оценки обеспечивает контроль использования интерфейсов ввода (вывода) средств вычислительной техники при подключении съемного машинного носителя информации путем реализации следующих процессов:

проверки наличия разрешения или запрета на использование интерфейса ввода (вывода) средства вычислительной техники при попытке подключения съемного машинного носителя информации;

разрешения или запрета использования подключаемого съемного машинного носителя информации по результатам выполненной проверки;

регистрации событий безопасности и записи информации аудита безопасности средства контроля подключения съемных машинных носителей информации.

2.2.3. Доступные аппаратные средства или программное обеспечение или программно-аппаратные средства, не входящие в объект оценки

В рамках настоящего ПЗ аппаратные средства или программное обеспечение или программно-аппаратные средства, не входящие в объект оценки, не рассматриваются.

2.3. Соглашения

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

Операция «**уточнение**» используется для добавления в компонент требований безопасности 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 компонента 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 настоящий ПЗ включен ряд требований безопасности, сформулированных в явном виде. Краткая форма имен компонентов требований, сформулированных в явном виде, содержит текст (ЕХТ).

Настоящий профиль защиты содержит ряд незавершенных операций над компонентами функциональных требований безопасности. Эти операции должны быть завершены в задании по безопасности для конкретной реализации СКН.

3. Утверждение соответствия

3.1. Утверждение о соответствии ИСО/МЭК 15408

Настоящий профиль защиты разработан в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» и ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

Настоящий профиль защиты содержит расширенные требования безопасности, разработанные в соответствии с правилами, установленными ГОСТ Р ИСО/МЭК 15408.

3.2. Утверждение о соответствии профилям защиты

Соответствие другим профилям защиты не требуется.

3.3. Обоснование соответствия

Соответствие другим профилям защиты не требуется.

3.4. Изложение соответствия

При разработке ЗБ и (или) других ПЗ на основе настоящего профиля защиты устанавливаются следующие типы соответствия:

«строгое» соответствие – если настоящий ПЗ является единственным ПЗ, утверждение о соответствии которому включено в ЗБ;

«демонстрируемое» соответствие – если ОО является комплексным продуктом (изделием), и в ЗБ включено утверждение о соответствии (дополнительно к настоящему ПЗ) другому (другим) ПЗ.

4. Цели безопасности

4.1. Цели безопасности для среды функционирования

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 (ИС), в котором (которой) 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 защита от осуществления действий, направленных на нарушение физической целостности СВТ, доступ к которым контролируется с применением СКН.

Цель для среды функционирования ОО-4

Поддержка аудита

Должна быть обеспечена поддержка средств аудита, используемых в ОО (расширенные возможности по хранению и анализу информации аудита безопасности), и предоставление для них надлежащего источника меток времени.

Цель для среды функционирования ОО-5

Идентификация и аутентификация

Должна быть обеспечена возможность идентификации и аутентификации администратора СКН, до предоставления ему возможности по управлению ОО, просмотру аудита безопасности и выполнения иных действий по администрированию ОО.

Цель для среды функционирования ОО-6

Управление атрибутами безопасности

Должна быть обеспечена возможность управления атрибутами безопасности компонентов СКН в СВТ (ИС) только уполномоченным администраторам ИС.

Цель для среды функционирования ОО-7**Обеспечение условий безопасного функционирования**

Должна быть обеспечена возможность контроля целостности программных компонентов СКН, поддержка доверенной связи между компонентами СКН. Должен осуществляться контроль вноса в контролируемую зону или выноса из контролируемой зоны съемных машинных носителей информации.

Цель для среды функционирования ОО-8**Требования к персоналу**

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

5. Определение расширенных компонентов

В данном разделе ПЗ представлены расширенные компоненты для средства контроля подключения съемных машинных носителей информации.

5.1. Определение расширенных компонентов функциональных требований безопасности

Для средств контроля подключения съемных машинных носителей информации определены следующие компоненты функциональных требований безопасности, сформулированные в явном виде в стиле компонентов из ГОСТ Р ИСО/МЭК 15408–2 (расширенные компоненты).

FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации

Иерархический для: Нет подчиненных компонентов.

FDP_IFC_EXT.3.1 Функции безопасности средства контроля съемных машинных носителей информации должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*] для [выбор: *съемных машинных носителей информации, специализированных съемных машинных носителей информации, используемых для хранения информации ограниченного доступа, [назначение: *другие типы подключаемых программно-аппаратных устройств*]*].

Зависимости: [FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации или FDP_IFF_EXT.8 Функции управления использованием специализированных съемных машинных носителей информации].

Управление: FDP_IFC_EXT.3

Действия по управлению не предусмотрены.

Аудит: FDP_IFC_EXT.3

Нет событий, для которых следует предусмотреть возможность аудита.

FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации

Иерархический для: Нет подчиненных компонентов.

FDP_IFF_EXT.7.1 Функции безопасности средства контроля съемных машинных носителей информации должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*], основанную на следующих типах данных функций безопасности средства контроля съемных машинных носителей информации: [выбор: *интерфейсы ввода (вывода) средств вычислительной техники, типы подключаемых внешних программно-аппаратных устройств, конкретные съемные машинные носители информации, список пользователей* [назначение: *другие типы данных функций безопасности средства контроля съемных машинных носителей информации, используемых для реализации политики управления использованием подключаемых съемных машинных носителей информации*]].

Зависимости: FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации.

Управление: FDP_IFF_EXT.7

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) Управление данными ФБО, используемыми при задании прав использования интерфейсов ввода (вывода), типов подключаемых внешних программно-аппаратных устройств, конкретных съемных машинных носителей информации.

Аудит: FDP_IFF_EXT.7

Если в ПЗ и (или) ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) Минимальный: разрешения на использование интерфейсов ввода (вывода), подключаемых внешних программно-аппаратных устройств конкретных типов, конкретных съемных машинных носителей информации.

б) Базовый: все решения по запросам на использование интерфейсов ввода (вывода), подключаемых внешних программно-аппаратных устройств конкретных типов, конкретных съемных машинных носителей информации.

в) Детализированный: специфические данные ФБО, используемые при принятии решений по запросам на использование интерфейсов ввода (вывода), подключаемых внешних программно-аппаратных устройств конкретных типов, конкретных съемных машинных носителей информации.

5.2. Определение расширенных компонентов требований доверия к безопасности

Для средств контроля подключения съемных машинных носителей информации определен следующий расширенный компонент требований доверия к безопасности AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации», сформулированный в явном виде в стиле компонентов из ГОСТ Р ИСО/МЭК 15408–3.

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации

Элементы действий заявителя

AMA_SIA_EXT.3.1D Заявитель должен представить материалы анализа влияния обновлений на безопасность средства контроля съемных машинных носителей информации.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность средства контроля съемных машинных носителей информации должны содержать краткое описание влияния обновлений на задание по безопасности, функции безопасности средства контроля съемных машинных носителей информации или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.3.2C Материалы анализа влияния обновлений на безопасность средства контроля съемных машинных носителей информации для обновлений, влияющих на безопасность, должны идентифицировать функции безопасности, компоненты средства контроля съемных машинных носителей информации, 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 контроля съемных машинных носителей информации.

Зависимости: отсутствуют.

6. Требования безопасности

В данном разделе ПЗ представлены функциональные требования безопасности и требования доверия к безопасности, 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 ОУД1, расширенного компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации». Требования безопасности на основе AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации» сформулированы в явном виде (расширение ГОСТ Р ИСО/МЭК 15408–3).

6.1. Требования безопасности для объекта оценки

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 6.1.

Таблица 6.1. - Функциональные компоненты, на которых основаны функциональные требования безопасности объекта оценки

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FDP_IFC_EXT.3	Политика управления использованием подключаемых съемных машинных носителей информации
FDP_IFF_EXT.7	Функции управления использованием подключаемых съемных машинных носителей информации
FMT_SMF.1	Спецификация функций управления
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_SMR.1	Роли безопасности

6.1.1. Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

- а) запуск и завершение выполнения функций аудита;
- б) все события, потенциально подвергаемые аудиту, на минимальном 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 (если применимо) и результат события (успешный или неуспешный);

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

Зависимости: FPT_STM.1 Надежные метки времени.

Замечания по применению:

В пункте б) FAU_GEN.1.1 выбран уровень аудита минимальный, с учетом этого разработчик ЗБ должен следовать инструкциям ГОСТ Р ИСО/МЭК 15408-2 по включению в FAU_GEN.1 событий согласно выбранному уровню аудита, используя пункты в рубрике «Аудит» для каждого функционального компонента из ГОСТ Р ИСО/МЭК 15408-2, включенного в ПЗ и (или) ЗБ, и каждого компонента ФТБ, определенного в подразделе 5.1 настоящего ПЗ. Разработчик ЗБ может дополнительно указать в пункте в) FAU_GEN.1.1 другие события, которые ОО потенциально способен подвергать аудиту.

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [назначение: *уполномоченные идентифицированные роли из состава ролей безопасности*] возможность читать [назначение: *список информации аудита*] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

Зависимости: FAU_GEN.1 Генерация данных аудита.

6.1.2. Защита данных пользователя (FDP)

FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации

FDP_IFC_EXT.3.1 ФБО должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*] для подключаемых произвольных съемных машинных носителей информации, [назначение: *другие типы подключаемых программно-аппаратных устройств*].

Зависимости: [FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации или FDP_IFF_EXT.8 Функции управления использованием специализированных съемных машинных носителей информации].

FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации

FDP_IFF_EXT.7.1 ФБО должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*], основанную на следующих типах данных ФБО: *интерфейсы ввода (вывода) средств вычислительной техники*, [назначение: *другие типы данных ФБО, используемых для реализации Политики управления использованием подключаемых съемных машинных носителей информации*].

Зависимости: FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации.

6.1.3. Управление безопасностью (FMT)

FMT_SMF.1 Спецификация функций управления

FMT_SMF.1.1 ФБО должны быть способны к выполнению следующих функций управления: [управление режимом выполнения функций безопасности, управление данными ФБО], [назначение: *список других функций управления безопасностью, предоставляемых ФБО*].

Зависимости: отсутствуют.

FMT_MTD.1 Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность [выбор: *изменение значений по умолчанию, запрос, модификация, удаление, очистка* [назначение: *другие операции*]] следующих данных [назначение: *список данных ФБО*] только [администраторами СКН].

Зависимости: FMT_SMR.1 Роли безопасности.

FMT_SMF.1 Спецификация функций управления.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли
[а) администратор СКН;
б) пользователь].

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

Зависимости: FIA_UID.1 Выбор момента идентификации.

6.1.4. Обоснование удовлетворения зависимостей функциональных требований безопасности

В таблице 6.2 представлены результаты удовлетворения зависимостей функциональных требований безопасности. 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 6.2 является справочным и содержит компоненты, определенные в ГОСТ Р ИСО/МЭК 15408–2 в описании компонентов требований, приведенных в столбце 1 таблицы 6.2, под рубрикой «Зависимости».

Столбец 3 таблицы 6.2. показывает, какие компоненты требований были включены в настоящий ПЗ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 6.2. Компоненты требований в столбце 3 таблицы 6.2. либо совпадают с компонентами в столбце 2 таблицы 6.2., либо иерархичны по отношению к ним.

Таблица 6.2. - Зависимости функциональных требований безопасности

Функциональный компонент	Зависимость в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 5.1 настоящего ПЗ	Удовлетворение зависимости
FAU_GEN.1	FPT_STM.1	Цель для среды функционирования ОО-4
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FDP_IFC_EXT.3	FDP_IFF_EXT.7 FDP_IFF_EXT.8	FDP_IFF_EXT.7
FDP_IFF_EXT.7	FDP_IFC_EXT.3	FDP_IFC_EXT.3
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMR.1	FIA_UID.1	Цель для среды функционирования ОО-5

Все зависимости включенных в ПЗ компонентов ФТБ удовлетворены.

6.2. Требования доверия к безопасности

Требования доверия к безопасности ОО взяты из ГОСТ Р ИСО/МЭК 15408–3 и образуют ОУД1, расширенный компонентом АМА_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации» (см. таблицу 6.3).

Таблица 6.3. – Требования доверия к безопасности объекта оценки

Класс доверия	Идентификатор компонентов доверия	Название компонента доверия
Разработка	ADV_FSP.1	Базовая функциональная спецификация
Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_PRE.1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC.1	Маркировка ОО
	ALC_CMS.1	Охват УК объекта оценки

Окончание таблицы 6.3.

Класс доверия	Идентификатор компонентов доверия	Название компонента доверия
Оценка задания по безопасности	ASE_CCL.1	Утверждения о соответствии
	ASE_ECD.1	Определение расширенных компонентов
	ASE_INT.1	Введение ЗБ
	ASE_OBJ.1	Цели безопасности для среды функционирования
	ASE_REQ.1	Установленные требования безопасности
	ASE_TSS.1	Краткая спецификация ОО
	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_VAN.1	Обзор уязвимостей
Обновление СКН	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации

6.2.1. Разработка (ADV)

ADV_FSP.1 Базовая функциональная спецификация

Зависимости: отсутствуют.

Элементы действий заявителя

ADV_FSP.1.1D Заявитель должен представить функциональную спецификацию.

ADV_FSP.1.2D Заявитель должен представить прослеживание функциональной спецификации к ФТБ.

Элементы содержания и представления свидетельств

ADV_FSP.1.1C В функциональной спецификации должны описываться назначение и метод использования для каждого из ИФБО, осуществляющих или поддерживающих выполнение ФТБ.

ADV_FSP.1.2C В функциональной спецификации должны быть идентифицированы все параметры, связанные с каждым ИФБО, осуществляющим или поддерживающим ФТБ.

ADV_FSP.1.3C В функциональной спецификации должно приводиться обоснование неявного категорирования интерфейсов как не влияющих на выполнение ФТБ.

ADV_FSP.1.4C В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий испытательной лаборатории

ADV_FSP.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.1.2E Испытательная лаборатория должна сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

6.2.2. AGD: Руководства

AGD_OPE.1 Руководство пользователя по эксплуатации

Зависимости: ADV_FSP.1 Базовая функциональная спецификация.

Элементы действий заявителя

AGD_OPE.1.1D Заявитель должен представить руководство пользователя по эксплуатации.

Элементы содержания и представления свидетельств

AGD_OPE.1.1C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.

AGD_OPE.1.2C В руководстве пользователя по эксплуатации в рамках каждой пользовательской роли должно быть представлено описание принципов безопасной работы с предоставленными в ОО интерфейсами.

AGD_OPE.1.3C В руководстве пользователя по эксплуатации должно быть представлено описание доступных для каждой пользовательской роли функций и интерфейсов, особенно всех параметров безопасности под управлением пользователя, с указанием безопасных значений, если это уместно.

AGD_OPE.1.4C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО.

AGD_OPE.1.5C В руководстве пользователя по эксплуатации должны быть идентифицированы все возможные режимы работы ОО (включая операции после сбоя и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования.

AGD_OPE.1.6C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть **приведено** описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ, **имеющих отношение к пользователю**.

AGD_OPE.1.7C Руководство пользователя по эксплуатации должно быть четким и обоснованным.

Элементы действий испытательной лаборатории

AGD_OPE1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_PRE.1 Подготовительные процедуры

Зависимости: отсутствуют.

Элементы действий заявителя

AGD_PRE.1.1D Заявитель должен предоставить ОО вместе с подготовительными процедурами.

Элементы содержания и представления свидетельств

AGD_PRE1.1C В подготовительных процедурах должны описываться все шаги, необходимые для безопасной приемки поставленного ОО в соответствии с процедурами поставки заявителя.

AGD_PRE1.2C В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки ОО, **реализации и оценки реализации всех функций безопасности среды функционирования ОО** в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.

Элементы действий испытательной лаборатории

AGD_PRE.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_PRE.1.2E Испытательная лаборатория должна использовать подготовительные процедуры для подтверждения того, что ОО может быть безопасно подготовлен к работе.

6.2.3. ALC: Поддержка жизненного цикла

ALC_CMS.1 Маркировка ОО

Зависимости: ALC_CMS.1 Охват УК ОО.

Элементы действий заявителя

ALC_CMS.1.1D Заявитель должен предоставить ОО и маркировку для ОО.

Элементы содержания и представления свидетельств

ALC_CMS.1.1C ОО должен быть помечен уникальной маркировкой.

Элементы действий испытательной лаборатории

ALC_CMS.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_CMS.1 Охват УК объекта оценки

Зависимости: отсутствуют.

Элементы действий заявителя

ALC_CMS.1.1D Заявитель должен представить список элементов конфигурации для ОО.

Элементы содержания и представления свидетельств

ALC_CMS.1.1C Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по ТДБ в ЗБ.

ALC_CMS.1.2C Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

Элементы действий испытательной лаборатории

ALC_CMS.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

6.2.4. ASE: Оценка задания по безопасности

ASE_CCL.1 Утверждения о соответствии

Зависимости:

ASE_INT.1 Введение ЗБ.

ASE_ECD.1 Определение расширенных компонентов.

ASE_REQ.1 Установленные требования безопасности.

Элементы действий заявителя

ASE_CCL.1.1D Заявитель должен представить «Утверждения о соответствии».

ASE_CCL.1.2D Заявитель должен представить «Обоснование утверждений о соответствии».

Элементы содержания и представления свидетельств

ASE_CCL.1.1C В «Утверждения о соответствии» должно быть включено «Утверждение о соответствии ИСО/МЭК 15408», которое определяет, для какой редакции ИСО/МЭК 15408 утверждается соответствие ЗБ и ОО.

ASE_CCL.1.2C В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ЗБ ИСО/МЭК 15408-2; ЗБ либо описывается как соответствующее требованиям ИСО/МЭК 15408-2, либо как содержащее расширенные по отношению к ИСО/МЭК 15408-2 требования.

ASE_CCL.1.3C В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ПЗ ИСО/МЭК 15408-3; ЗБ либо описывается как соответствующее требованиям ИСО/МЭК 15408-3, либо как содержащее расширенные по отношению к ИСО/МЭК 15408-3 требования.

ASE_CCL.1.4C «Утверждение о соответствии ИСО/МЭК 15408» должно согласовываться с «Определением расширенных компонентов».

ASE_CCL.1.5C В «Утверждении о соответствии» должны быть идентифицированы все ПЗ и пакеты требований безопасности, о соответствии которым утверждается в ЗБ.

ASE_CCL.1.6C В «Утверждении о соответствии ЗБ пакету требований» должно приводиться описание любого соответствия ЗБ некоторому пакету требований; ЗБ либо описывается как

соответствующее пакету требований, либо как содержащее расширенные по отношению к пакету требования.

ASE_CCL.1.7C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что тип ОО согласуется с типом ОО в тех ПЗ, о соответствии которым утверждается.

ASE_CCL.1.8C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Определения проблемы безопасности» согласуется с изложением «Определения проблемы безопасности» в тех ПЗ, о соответствии которым утверждается.

ASE_CCL.1.9C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Целей безопасности» согласуется с изложением «Целей безопасности» в тех ПЗ, о соответствии которым утверждается.

ASE_CCL.1.10C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Требований безопасности» согласуется с изложением «Требований безопасности» в тех ПЗ, о соответствии которым утверждается.

Элементы действий испытательной лаборатории

ASE_CCL.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_ECD.1 Определение расширенных компонентов

Зависимости: отсутствуют.

Элементы действий заявителя

ASE_ECD.1.1D Заявитель должен представить изложение «Требований безопасности».

ASE_ECD.1.2D Заявитель должен представить «Определение расширенных компонентов».

Элементы содержания и представления свидетельств

ASE_ECD.1.1C В изложении «Требований безопасности» должны быть идентифицированы все расширенные требования безопасности.

ASE_ECD.1.2C В «Определении расширенных компонентов» должен определяться расширенный компонент для каждого расширенного требования безопасности.

ASE_ECD.1.3C В «Определении расширенных компонентов» должно указываться, как каждый расширенный компонент связан с существующими компонентами, семействами и классами ИСО/МЭК 15408.

ASE_ECD.1.4C В «Определении расширенных компонентов» должны использоваться в качестве модели представления компоненты, семейства, классы и методология ИСО/МЭК 15408.

ASE_ECD.1.5C Расширенные компоненты должны состоять из измеримых объективных элементов, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.

Элементы действий испытательной лаборатории

ASE_ECD.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_ECD.1.2E Испытательная лаборатория должна подтвердить, что ни один из расширенных компонентов не может быть четко выражен с использованием существующих компонентов.

ASE_INT.1 Введение ЗБ

Зависимости: отсутствуют.

Элементы действий заявителя

ASE_INT.1.1D Разработчик ЗБ должен представить «Введение ЗБ».

Элементы содержания и представления свидетельств

ASE_INT.1.1C «Введение ЗБ» должно содержать «Ссылку на ЗБ», «Ссылку на ОО», «Аннотацию ОО» и «Описание ОО».

ASE_INT.1.2C «Ссылка на ЗБ» должна однозначно идентифицировать ЗБ.

ASE_INT.1.3C «Ссылка на ОО» должна однозначно идентифицировать ОО.

ASE_INT.1.4C В «Аннотации ОО» должна быть представлена краткая информация о его использовании и основных функциональных возможностях безопасности ОО.

ASE_INT.1.5C В «Аннотации ОО» должен быть идентифицирован тип ОО.

ASE_INT.1.6C В «Аннотации ОО» должны быть идентифицированы любые не входящие в ОО аппаратные, программные, а также программно-аппаратные средства, требуемые ОО.

ASE_INT.1.7C «Описание ОО» должно включать описание физических границ ОО.

ASE_INT.1.8C «Описание ОО» должно включать описание логических границ ОО.

Элементы действий испытательной лаборатории

ASE_INT.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_INT.1.2E Испытательная лаборатория должна подтвердить, что «Ссылка на ОО», «Аннотация ОО» и «Описание ОО» не противоречат друг другу.

ASE_OBJ.1 Цели безопасности для среды функционирования

Зависимости: отсутствуют.

Элементы действий заявителя

ASE_OBJ.1.1D Заявитель должен представить изложение «Целей безопасности».

Элементы содержания и представления свидетельств

ASE_OBJ.1.1C Изложение «Целей безопасности» должно включать в себя описание целей безопасности для среды функционирования ОО.

Элементы действий испытательной лаборатории

ASE_OBJ.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_REQ.1 Установленные требования безопасности

Зависимости: ASE_ECD.1 Определение расширенных компонентов.

Элементы действий заявителя

ASE_REQ.1.1D Заявитель должен представить изложение «Требований безопасности».

ASE_REQ.1.2D Заявитель должен представить «Обоснование требований безопасности».

Элементы содержания и представления свидетельств

ASE_REQ.1.1C Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.

ASE_REQ.1.2C Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.

ASE_REQ.1.3C В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.

ASE_REQ.1.4C Все операции должны выполняться правильно.

ASE_REQ.1.5C Каждая зависимость от требований безопасности должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения данной зависимости.

ASE_REQ.1.6C Изложение «Требований безопасности» должно быть внутренне непротиворечивым.

Элементы действий испытательной лаборатории

ASE_REQ.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_TSS.1 Краткая спецификация ОО

Зависимости: ASE_INT.1 Введение ЗБ.

ASE_REQ.1 Установленные требования безопасности.

ADV_FSP.1 Базовая функциональная спецификация.

Элементы действий заявителя

ASE_TSS.1.1D Заявитель должен представить краткую спецификацию ОО.

Элементы содержания и представления свидетельств

ASE_TSS.1.1C Краткая спецификация ОО должна описывать, каким образом ОО выполняет каждое ФТБ.

Элементы действий испытательной лаборатории

ASE_TSS.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_TSS.1.2E Испытательная лаборатория должна подтвердить, что краткая спецификация ОО не противоречит «Аннотации ОО» и «Описанию ОО».

6.2.5. АТЕ: Тестирование

АТЕ_IND.1 Независимое тестирование на соответствие

Зависимости: ADV_FSP.1 Базовая функциональная спецификация.
AGD_OPE.1 Руководство пользователя по эксплуатации.
AGD_PRE.1 Подготовительные процедуры.

Элементы действий заявителя

АТЕ_IND.1.1D Заявитель должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

АТЕ_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий испытательной лаборатории

АТЕ_IND.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АТЕ_IND.1.2E Испытательная лаборатория должна протестировать подмножество ФБО так, чтобы подтвердить, что ФБО функционируют в соответствии со спецификациями.

6.2.6. АВА: Оценка уязвимостей

АВА_VAN.1 Обзор уязвимостей

Зависимости: ADV_FSP.1 Базовая функциональная спецификация.
AGD_OPE.1 Руководство пользователя по эксплуатации.
AGD_PRE.1 Подготовительные процедуры.

Элементы действий заявителя

АВА_VAN.1.1D Заявитель должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

АВА_VAN.1.1C ОО должен быть пригоден для тестирования.

Элементы действий испытательной лаборатории

АВА_VAN.1.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АВА_VAN.1.2E Испытательная лаборатория должна выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA_VAN.1.3E Испытательная лаборатория должна провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим Базовым потенциалом нападения.

6.2.7. Требования к объекту оценки, сформулированные в явном виде

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации

Элементы действий заявителя

AMA_SIA_EXT.3.1D Заявитель должен представить материалы анализа влияния обновлений на безопасность средства контроля съемных машинных носителей информации.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность средства контроля съемных машинных носителей информации должны содержать краткое описание влияния обновлений на задание по безопасности, функции безопасности средства контроля съемных машинных носителей информации или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.3.2C Материалы анализа влияния обновлений на безопасность средства контроля съемных машинных носителей информации для обновлений, влияющих на безопасность, должны идентифицировать функции безопасности, компоненты средства контроля съемных машинных носителей информации, 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 контроля съемных машинных носителей информации.
