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 ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ

ИТ.СКН.П4.ПЗ

МОСКВА
2014

Содержание

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 четвертого класса защиты.
Тип СКН:	Средство контроля подключения съемных машинных носителей информации.
Класс защиты:	Четвертый.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.СКН.П4.ПЗ.
Идентификация ОО:	Средство контроля подключения съемных машинных носителей информации.
Уровень доверия:	Оценочный уровень доверия 3 (ОУД3), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ADV_FSP.4 «Полная функциональная спецификация», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентом AMA_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, ОУД3.

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, типов подключаемых внешних программно-аппаратных устройств и конкретных 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;

управление параметрами СКН;

контроль подключения съемных машинных носителей информации;

аудит безопасности СКН;

сигнализация 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 работой (режимами выполнения функций безопасности) СКН;

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

требования к контролю подключения съемных машинных носителей информации;

требования по предупреждению о событиях, связанных с нарушением безопасности;

требования к аудиту безопасности СКН.

Функциональные требования безопасности для СКН 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 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, типов подключаемых внешних программно-аппаратных устройств, конкретных съемных машинных носителей информации;

возможность со стороны администраторов СКН управлять данными (данными средства контроля подключения съемных машинных носителей информации), используемыми функциями безопасности средства контроля подключения 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 защиты от несанкционированной модификации данных средства контроля подключения съемных машинных носителей информации при передаче между программным обеспечением управления средствами контроля подключения съемных машинных носителей информации и программным обеспечением взаимодействия с подключаемыми съемными машинными носителями информации;

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;

возможность реагирования при обнаружении событий, указывающих на возможное нарушение безопасности;

возможность выборочного просмотра данных аудита.

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 средств контроля подключения съемных машинных носителей информации образуют оценочный уровень доверия 3 (ОУД3), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ADV_FSP.4 «Полная функциональная спецификация», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков» и AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентом AMA_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 и требования 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, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей 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;

проверки наличия разрешения или запрета на использование соответствующего типа подключаемых внешних программно-аппаратных устройств при наличии разрешения (отсутствия запрета) на использование интерфейса ввода (вывода) средства вычислительной техники;

проверки наличия разрешения или запрета на подключение конкретного съемного машинного носителя информации при наличии разрешения (отсутствия запрета) на подключение соответствующего типа внешних программно-аппаратных устройств;

разрешения или запрета использования подключаемого съемного машинного носителя информации по результатам выполненных проверок;

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 (EXT).

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 (помимо настоящему ПЗ) другому (другим) ПЗ.

4. Определение проблемы безопасности

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

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

политики безопасности организации, которую должен выполнять ОО;

предположений безопасности (обязательных условий безопасного использования ОО).

4.1. Угрозы безопасности информации

4.1.1. Угрозы, которым должен противостоять объект оценки

В настоящем ПЗ определены следующие угрозы, которым необходимо противостоять средствами ОО.

Угроза - 1

1. Аннотация угрозы – подключение к информационной системе внутренними и (или) внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из информационной системы.

2. Источники угрозы – внутренний нарушитель (пользователь информационной системы), внешний нарушитель (лицо, не являющееся пользователем информационной системы).

3. Способ реализации угрозы – подключение к средству вычислительной техники съемных машинных носителей информации, незарегистрированных в информационной системе и (или) не предназначенных для использования на конкретном интерфейсе ввода (вывода) средства вычислительной техники, и (или) не отнесенных к разрешенному типу, и (или) не отнесенных к разрешенным; несанкционированная запись защищаемой информации на подключенный съемный машинный носитель информации.

4. Используемые уязвимости – отсутствие или недостаточность мер контроля за использованием съемных машинных носителей информации в информационной системе.

5. Вид информационных ресурсов, потенциально подверженных угрозе – защищаемая информация, обрабатываемая в информационной системе; другие информационные ресурсы информационной системы.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с защищаемой информацией, обрабатываемой в информационной системе; нарушение режимов функционирования информационной системы.

Угроза - 2

1. Аннотация угрозы – подключение к информационной системе внутренними и (или) внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей загрузкой в информационную систему с этих съемных машинных носителей информации вредоносного ПО.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированные (преднамеренные, непреднамеренные) действия, направленные на подключение к ИС, загрузка в информационную систему с подключенного съемного машинного носителя информации вредоносного программного обеспечения.

4. Используемые уязвимости – наличие неконтролируемых интерфейсов, недостатки настройки механизмов защиты, наличие вредоносного программного обеспечения на незарегистрированных съемных машинных носителях информации.

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

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

7. Последствия реализации угрозы – нарушение режимов функционирования информационной системы за счет внедрения вредоносного программного обеспечения; недоступность информационных ресурсов информационной системы.

4.1.2. Угрозы, которым противостоит среда

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

Угроза среды-1

1. Аннотация угрозы – нарушение целостности программных компонентов СКН.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель, программное воздействие.

3. Способ реализации угрозы – действия, направленные на несанкционированные изменения целостности технических средств и программного обеспечения компонентов СКН, установку программных закладок.

4. Используемые уязвимости – недостатки механизмов управления и настройки ИС и недостатки, связанные с возможностью осуществления доступа к СВТ, в том числе с использованием незащищенных каналов связи.

5. Вид информационных ресурсов, потенциально подверженных угрозе – программные компоненты СКН.

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

7. Последствия реализации угрозы – нарушение целостности компонентов СКН, несанкционированный доступ к ресурсам ИС, нарушение режимов функционирования СКН.

Угроза среды-2

1. Аннотация угрозы – отключение компонентов СКН.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – несанкционированные действия, направленные на отключение компонентов СКН с использованием штатных и нештатных средств.

4. Используемые уязвимости – недостатки механизмов управления доступом, физической защиты СВТ, недостатки контроля за действиями пользователей.

5. Вид информационных ресурсов, потенциально подверженных угрозе – ПО СКН.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Последствия реализации угрозы – нарушение режимов функционирования СКН.

Угроза среды-3

1. Аннотация угрозы – несанкционированное изменение конфигурации (состава компонентов и их настроек) средств контроля съемных машинных носителей информации.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – действия, направленные на изменение параметров (конфигурации, состава компонентов и их настроек) СКН.

4. Используемые уязвимости – недостатки механизмов защиты программного обеспечения, поддерживающих возможность взаимодействия с СКН в СВТ и через механизм обновления программного обеспечения средств СКН.

5. Вид информационных ресурсов, потенциально подверженных угрозе – ПО СКН.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

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

4.2. Политика безопасности организации

Объект оценки должен выполнять приведенные ниже правила политики безопасности организации.

Политика безопасности-1

Должно осуществляться разграничение доступа к управлению СКН на основе ролей уполномоченных лиц.

Политика безопасности-2

Должно осуществляться управление со стороны уполномоченных лиц режимами выполнения функций безопасности СКН.

Политика безопасности-3

Управление параметрами СКН, которые влияют на выполнение функций безопасности СКН, должно осуществляться только уполномоченными на это лицами.

Политика безопасности-4

Должен обеспечиваться контроль использования интерфейсов ввода (вывода) в СВТ при подключении съемных машинных носителей информации.

Политика безопасности-5

Должен обеспечиваться контроль типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации.

Политика безопасности-6

Должны быть обеспечены надлежащие механизмы регистрации и предупреждения (сигнализации) о событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации должны предоставлять уполномоченным на это лицам возможность выборочного ознакомления с информацией о произошедших событиях.

4.3. Предположения безопасности

Предположения, связанные с физическими аспектами среды функционирования

Предположение-1

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

Предположения по отношению к аспектам связности среды функционирования

Предположение-2

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

Предположение-3

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

Предположения, связанные с персоналом среды функционирования

Предположение-4

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

5. Цели безопасности

5.1. Цели безопасности для объекта оценки

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Разграничение доступа к управлению СКН

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

Цель безопасности-2

Управление работой СКН

Объект оценки должен обеспечивать возможность управления со стороны уполномоченных лиц с учетом их ролей режимами выполнения функций безопасности СКН.

Цель безопасности-3

Управление параметрами СКН

Объект оценки должен обеспечивать возможность управления параметрами СКН, которые влияют на выполнение функций безопасности СКН, со стороны уполномоченных лиц с учетом их ролей.

Цель безопасности-4

Контроль интерфейсов

Объект оценки должен обеспечивать контроль использования интерфейсов ввода (вывода) в СВТ.

Цель безопасности-5

Контроль устройств

Объект оценки должен обеспечивать контроль типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации.

Цель безопасности-6

Аудит безопасности СКН

Объект оценки должен обеспечивать надлежащие механизмы регистрации и предупреждения (сигнализации) о событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации должны предоставлять уполномоченным лицам с учетом их ролей возможность полного или выборочного ознакомления с информацией о произошедших событиях.

5.2. 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.

5.3. Обоснование целей безопасности

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

В таблице 5.1. приведено отображение целей безопасности для ОО на угрозы и политику безопасности организации.

Таблица 5.1. – Отображение целей безопасности для объекта оценки 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**	
Угроза-2	**X**	**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 управлению СКН со стороны уполномоченных лиц.

Цель безопасности-2

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

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-3**, так как обеспечивает

возможность управления параметрами СКН, влияющими на функции безопасности СКН.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-4**, так как обеспечивает возможность контроля интерфейсов ввода (вывода) в СВТ.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-1** и реализацией политики безопасности **Политика безопасности-5**, так как обеспечивает возможность контроля подключаемых типов внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-6**, так как обеспечивает возможность сигнализации уполномоченным лицам о нарушениях, возможность регистрации и учета информации о событиях, относящихся к возможным нарушениям безопасности.

6. Определение расширенных компонентов

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

6.1. 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.

6.2. 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.

7. 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 ОУД3, усиленного компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ADV_FSP.4 «Полная функциональная спецификация», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей» и 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).

7.1. Функциональные требования безопасности

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 7.1.

Таблица 7.1. - Функциональные компоненты, на которых основаны функциональные требования безопасности объекта оценки

Идентификатор компонента требований	Название компонента требований
FAU_ARP.1	Сигналы нарушения безопасности
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FAU_SAR.3	Выборочный 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_MTD.1	Управление данными ФБО
FMT_SMR.1	Роли безопасности
FPT_ITT.1	Базовая защита внутренней передачи данных функций безопасности средства контроля съемных машинных носителей информации

7.1.1. Аудит безопасности (FAU)

FAU_ARP.1 Сигналы нарушения безопасности

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

Зависимости: FAU_SAA.1 Анализ потенциального нарушения.

Замечания по применению:

Разработчик ЗБ, кроме информирования администратора СКН, может перечислить и другие действия при обнаружении возможного нарушения безопасности. В этом случае разработчику ЗБ необходимо будет четко определить содержание, последовательность и результаты 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 *базовом* 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 базовый, 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 6.1 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.

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны предоставлять возможность использовать [назначение: *методы выбора и (или) упорядочения*] данных аудита, основанные на [назначение: *критерии с логическими отношениями*].

Зависимости: FAU_SAR.1 Просмотр аудита.

Замечания по применению: В ЗБ при выполнении второй операции «назначение» в FAU_SAR.3.1 следует указать критерии, основанные на комбинации атрибутов.

7.1.2. 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, типы подключаемых внешних программно-аппаратных устройств, конкретные съемные носители информации*, [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.

7.1.3. 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_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны предоставлять возможность [выбор: *определять режим выполнения, отключать, подключать, модифицировать режим выполнения*] функций [назначение: *список функций*] только [администраторами СКН].

Зависимости: FMT_SMR.1 Роли безопасности.
FMT_SMF.1 Спецификация функций управления.

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.

7.1.4. Защита ФБО (FPT)

FPT_ITT.1 Базовая защита внутренней передачи данных ФБО

FPT_ITT.1.1 ФБО должны защитить **данные средства контроля съемных машинных носителей информации** от ***несанкционированной*** *модификации* при их передаче между **программным обеспечением управления средствами контроля съемных машинных носителей информации и программным обеспечением взаимодействия с подключаемыми съемными машинными носителями информации.**

Зависимости: отсутствуют.

7.2. Требования доверия к безопасности

Требования доверия к безопасности ОО взяты из ГОСТ Р ИСО/МЭК 15408–3 и образуют ОУД3, усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ADV_FSP.4 «Полная функциональная спецификация», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей» и расширенный компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации» (см. таблицу 7.2.).

Таблица 7.2. – Требования доверия к безопасности объекта оценки

Класс доверия	**Идентификатор компонента доверия**	**Название компонента доверия**
Разработка	ADV_ARC.1	Описание архитектуры безопасности
	ADV_FSP.4	Полная функциональная спецификация
	ADV_IMP.2*	Полное отображение представления реализации ФБО
	ADV_TDS.3	Базовый модульный проект
Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_PRE.1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC.4	Поддержка генерации, процедуры приемки и автоматизация
	ALC_CMS.3	Охват УК представления реализации
	ALC_DEL.1	Процедуры поставки
	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR.1	Базовое устранение недостатков
	ALC_LCD.1	Определенная заявителем модель жизненного цикла
	ALC_TAT.1	Полностью определенные инструментальные средства разработки
Оценка задания по безопасности	ASE_CCL.1	Утверждения о соответствии
	ASE_ECD.1	Определение расширенных компонентов
	ASE_INT.1	Введение ЗБ
	ASE_OBJ.2	Цели безопасности
	ASE_REQ.2	Производные требования безопасности
	ASE_SPD.1	Определение проблемы безопасности
	ASE_TSS.1	Краткая спецификация ОО
Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.1	Тестирование: базовый проект
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_VAN.4*	Методический анализ уязвимостей

Окончание таблицы 7.2.

Класс доверия	Идентификатор компонента доверия	Название компонента доверия
Обновление СКН	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации
* – Отмечены компоненты, конкретизированные в настоящем ПЗ для обеспечения преемственности требованиям по контролю отсутствия недекларированных возможностей, изложенных в руководящем документе «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации: Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999).		

7.2.1. Разработка (ADV)

ADV_ARC.1 Описание архитектуры безопасности

Зависимости: ADV_FSP.1 Базовая функциональная спецификация.
ADV_TDS.1 Базовый проект.

Элементы действий заявителя

ADV_ARC.1.1D Заявитель должен спроектировать ОО и обеспечить реализацию проекта таким образом, чтобы свойства безопасности ФБО невозможно было обойти.

ADV_ARC.1.2D Заявитель должен спроектировать ФБО и обеспечить их реализацию таким образом, чтобы ФБО обеспечивали собственную защиту от вмешательства недоверенных сущностей.

ADV_ARC.1.3D Заявитель должен предоставить «Описание архитектуры безопасности» ФБО.

Элементы содержания и представления свидетельств

ADV_ARC.1.1C Уровень детализации «Описания архитектуры безопасности» должен соответствовать представленному в проектной документации по ОО описанию абстракций (элементов представления ОО), осуществляющих выполнение ФТБ.

ADV_ARC.1.2C В «Описание архитектуры безопасности» должно быть включено описание доменов безопасности, обеспеченных согласованностью ФБО с ФТБ.

ADV_ARC.1.3C «Описание архитектуры безопасности» должно предоставлять информацию о том, насколько процесс инициализации ФБО является защищенным.

ADV_ARC.1.4C В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО обеспечивают собственную защиту от вмешательства.

ADV_ARC.1.5C В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО не допускают возможности обхода функциональных возможностей, осуществляющих выполнение ФТБ.

Элементы действий испытательной лаборатории

ADV_ARC.1.1E Испытательная лаборатория должна подтвердить, что

представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.4 Полная функциональная спецификация

Зависимости: ADV_TDS.1 Базовый проект

Элементы действий заявителя

ADV_FSP.4.1D Заявитель должен представить функциональную спецификацию.

ADV_FSP.4.2D Заявитель должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления свидетельств

ADV_FSP.4.1C В функциональной спецификации должны быть полностью представлены ФБО.

ADV_FSP.4.2C В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV_FSP.4.3C В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV_FSP.4.4C В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.

ADV_FSP.4.5C Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.

ADV_FSP.4.6C В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий испытательной лаборатории

ADV_FSP.4.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.4.2E Испытательная лаборатория должна сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

ADV_IMP.2 Полное отображение представления реализации ФБО

Зависимости: ADV_TDS.3 Базовый модульный проект.
ALC_TAT.1 Полностью определенные инструментальные средства разработки.
ALC_CMC.5 Расширенная поддержка.

Элементы действий заявителя

ADV_IMP.2.1D Заявитель должен обеспечить испытательной лаборатории доступ к представлению реализации для всех ФБО **на уровне исходных текстов всего программного обеспечения, входящего в состав ОО, а также указать в документации значения**

контрольных сумм файлов с исходными текстами ПО и контрольных сумм загрузочных модулей ПО.

ADV_IMP.2.2D Заявитель должен обеспечить прослеживание **загрузочных модулей к представлению реализации, а также** всего представления реализации к описанию проекта ОО.

Элементы содержания и представления свидетельств

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

ADV_IMP.2.2C Представление реализации должно быть изложено в том виде, какой используется персоналом, занимающимся разработкой.

ADV_IMP.2.3C В прослеживании **между загрузочными модулями и представлением реализации, а также** между всем представлением реализации и описанием проекта ОО должно быть продемонстрировано их соответствие.

Элементы действий испытательной лаборатории

ADV_IMP.2.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств, **в том числе на основе результатов:**

контроля исходного состояния ПО;

контроля полноты и отсутствия избыточности исходных текстов на уровне файлов и на уровне функциональных объектов (процедур);

контроля соответствия исходных текстов ПО его объектному (загрузочному) коду.

Замечания по применению: 1. В ADV_IMP.2.1E контроль исходного состояния ПО предусматривает расчет уникальных значений контрольных сумм файлов с исходными текстами программ, входящих в состав ПО. Контрольные суммы должны рассчитываться для каждого файла.

2. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов и на уровне функциональных объектов (процедур) предусматривает анализ свидетельства, предоставленного заявителем в соответствии с ADV_IMP.2.3C, для подтверждения, что все ФБО представлены в исходных текстах ПО, а также что для всех файлов исходных текстов в проекте имеется соответствующее описание реализуемых ФБО.

3. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду предусматривает экспериментальное установление возможности получения путем проведения компиляции (трансляции) исходных текстов в объектный (загрузочный) код, однозначно соответствующий объектному (загрузочному) коду исполняемых модулей, составляющих исследуемое программное обеспечение (применимо только для

компилируемых (транслируемых) языков программирования).

ADV_TDS.3 Базовый модульный проект

Зависимости: ADV_FSP.4 Полная функциональная спецификация.

Элементы действий заявителя

ADV_TDS.3.1D Заявитель должен представить проект ОО.

ADV_TDS.3.2D Заявитель должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Элементы содержания и представления свидетельств

ADV_TDS.3.1C В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV_TDS.3.2C В проекте должно приводиться описание структуры ОО на уровне модулей.

ADV_TDS.3.3C В проекте должны быть идентифицированы все подсистемы ФБО.

ADV_TDS.3.4C В проекте должно приводиться описание каждой из подсистем ФБО.

ADV_TDS.3.5C В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV_TDS.3.6C В проекте должно быть осуществлено прослеживание подсистем ФБО с модулями ФБО.

ADV_TDS.3.7C В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV_TDS.3.8C В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.

ADV_TDS.3.9C В проекте должен быть описан каждый поддерживающий и не влияющий на выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV_TDS.3.10C В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий испытательной лаборатории

ADV_TDS.3.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_TDS.3.2E Испытательная лаборатория должна сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

7.2.2. 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 сбоев 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 представить 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.

7.2.3. ALC: Поддержка жизненного цикла

ALC_CMC.4 Поддержка генерации, процедуры приемки и автоматизация

Зависимости: ALC_CMS.1 Охват УК ОО.
ALC_DVS.1 Идентификация мер безопасности.
ALC_LCD.1 Определенная заявителем модель жизненного цикла.

Элементы действий заявителя

ALC_CMC.4.1D Заявитель должен предоставить ОО и маркировку для ОО.

ALC_CMC.4.2D Заявитель должен предоставить документацию УК.

ALC_CMC.4.3D Заявитель должен использовать систему УК.

Элементы содержания и представления свидетельств

ALC_CMC.4.1C ОО должен быть помечен уникальной маркировкой.

ALC_CMC.4.2C В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.

ALC_CMC.4.3C В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.

ALC_CMC.4.4C В системе УК должны быть предусмотрены такие автоматизированные меры, при применении которых в элементы конфигурации могут быть внесены только санкционированные изменения.

ALC_CMC.4.5C Система УК должна поддерживать производство ОО автоматизированными средствами.

ALC_CMC.4.6C Документация УК должна включать в себя план УК.

ALC_CMC.4.7C В плане УК должно быть описание того, каким образом система УК используется для разработки ОО.

ALC_CMC.4.8C План УК должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части ОО.

ALC_CMC.4.9C В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.

ALC_CMC.4.10C В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.

Элементы действий испытательной лаборатории

ALC_CMC.4.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_CMS.3 Охват УК представления реализации

Зависимости: отсутствуют

Элементы действий заявителя

ALC_CMS.3.1D Заявитель должен представить список элементов конфигурации для ОО.

Элементы содержания и представления свидетельств

ALC_CMS.3.1C Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по требованиям доверия к безопасности, части, которые входят в состав ОО, а также представление реализации.

ALC_CMS.3.2C Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC_CMS.3.3C Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан заявитель.

Элементы действий испытательной лаборатории

ALC_CMS.3.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_DEL.1 Процедуры поставки

Зависимости: отсутствуют.

Элементы действий заявителя

ALC_DEL.1.1D Заявитель должен задокументировать процедуры поставки ОО или его частей потребителю.

ALC_DEL.1.2D Заявитель должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ALC_DEL.1.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержания безопасности при распространении версий ОО потребителю.

Элементы действий испытательной лаборатории

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

ALC_DVS.1 Идентификация мер безопасности

Зависимости: отсутствуют.

Элементы действий заявителя

ALC_DVS.1.1D Заявитель должен представить документацию по безопасности разработки.

Элементы содержания и представления свидетельств

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

Элементы действий испытательной лаборатории

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

ALC_DVS.1.2E Испытательная лаборатория должна подтвердить, что меры безопасности применяются.

ALC_FLR.1 Базовое устранение недостатков

Зависимости: отсутствуют.

Элементы действий заявителя

ALC_FLR.1.1D Заявитель должен предоставить процедуры устранения недостатков, предназначенные для заявителей ОО.

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 каждом релизе ОО.

ALC_FLR.1.2C Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.

ALC_FLR.1.3C Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.

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 испытательной лаборатории

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

ALC_LCD.1 Определенная заявителем модель жизненного цикла

Зависимости: отсутствуют.

Элементы действий заявителя

ALC_LCD.1.1D Заявитель должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.

ALC_LCD.1.2D Заявитель должен представить документацию по определению жизненного цикла.

Элементы содержания и представления свидетельств

ALC_LCD.1.1C Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.

ALC_LCD.1.2C Модель жизненного цикла должна обеспечить необходимый контроль над разработкой и сопровождением ОО.

Элементы действий испытательной лаборатории

ALC_LCD.1.1E Испытательная лаборатория должна 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 заявителя

ALC_TAT.1.1D Заявитель должен идентифицировать каждое инструментальное средство, используемое для разработки ОО.

ALC_TAT.1.2D Заявитель должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

Элементы содержания и представления свидетельств

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

ALC_TAT.1.2C В документации по инструментальным средствам разработки должны быть однозначно определены значения всех языковых конструкций, используемых в реализации.

ALC_TAT.1.3C В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.

Элементы действий испытательной лаборатории

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

7.2.4. 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 Задания по безопасности

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.2 Цели безопасности

Зависимости: ASE_SPD.1 Определение проблемы безопасности.

Элементы действий заявителя

ASE_OBJ.2.1D Заявитель должен представить «Определение целей безопасности».

ASE_OBJ.2.2D Заявитель должен представить «Обоснование целей безопасности».

Элементы содержания и представления свидетельств

ASE_OBJ.2.1C Изложение «Целей безопасности» должно включать в себя описание целей безопасности для ОО и для среды функционирования ОО.

ASE_OBJ.2.2C В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, и к ПБОр, на осуществление которых направлена эта цель безопасности.

ASE_OBJ.2.3C В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на

противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, а также к предположениям, поддерживаемым данной целью безопасности.

ASE_OBJ.2.4C В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на противостояние всем идентифицированным угрозам.

ASE_OBJ.2.5C В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на осуществление всех ПБОр.

ASE_OBJ.2.6C В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности для среды функционирования поддерживают все предположения.

Элементы действий испытательной лаборатории

ASE_OBJ.2.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_REQ.2 Производные требования безопасности

Зависимости: ASE_OBJ.2 Цели безопасности.
ASE_ECD.1 Определение расширенных компонентов.

Элементы действий заявителя

ASE_REQ.2.1D Заявитель должен представить «Определение требований безопасности».

ASE_REQ.2.2D Заявитель должен представить «Обоснование требований безопасности».

Элементы содержания и представления свидетельств

ASE_REQ.2.1C Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.

ASE_REQ.2.2C Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, использующиеся в ФТБ и ТБД, должны быть определены.

ASE_REQ.2.3C В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.

ASE_REQ.2.4C Все операции должны выполняться правильно.

ASE_REQ.2.5C Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения зависимости.

ASE_REQ.2.6C В «Обосновании требований безопасности» должно быть представлено прослеживание каждого ФТБ к целям безопасности для ОО.

ASE_REQ.2.7C В «Обосновании требований безопасности» должно быть продемонстрировано, что ФТБ обеспечивают выполнение всех

целей безопасности для ОО.

ASE_REQ.2.8C В «Обосновании требований безопасности» должно приводиться пояснение того, почему выбраны определенные ТДБ.

ASE_REQ.2.9C Изложение «Требований безопасности» должно быть внутренне непротиворечивым.

Элементы действий испытательной лаборатории

ASE_REQ.2.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_SPD.1 Определение проблемы безопасности

Зависимости: отсутствуют.

Элементы действий заявителя

ASE_SPD.1.1D Заявитель должен представить «Определение проблемы безопасности».

Элементы содержания и представления свидетельств

ASE_SPD.1.1C «Определение проблемы безопасности» должно включать в себя описание угроз.

ASE_SPD.1.2C Описание всех угроз должно проводиться в терминах источника угрозы, активов и негативного действия.

ASE_SPD.1.3C В «Определение проблемы безопасности» должно быть включено описание ПБОр.

ASE_SPD.1.4C «Определение проблемы безопасности» должно содержать описание предположений относительно среды функционирования ОО.

Элементы действий испытательной лаборатории

ASE_SPD.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».

7.2.5. ATE: Тестирование

ATE_COV.2 Анализ покрытия

Зависимости: ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации.
ATE_FUN.1 Функциональное тестирование.

Элементы действий заявителя

ATE_COV.2.1D Заявитель должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

ATE_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.

ATE_COV.2.2C Анализ покрытия тестами должен демонстрировать, что все ИФБО из функциональной спецификации были подвергнуты тестированию.

Элементы действий испытательной лаборатории

ATE_COV.2.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_DPT.1 Тестирование: базовый проект

Зависимости: ADV_ARC.1 Описание архитектуры безопасности.
ADV_TDS.2 Архитектурный проект.
ATE_FUN.1 Функциональное тестирование.

Элементы действий заявителя

ATE_DPT.1.1D Заявитель должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.1.1C Анализ глубины тестирования должен демонстрировать соответствие между тестами из тестовой документации и подсистемами ФБО из проекта ОО.

ATE_DPT.1.2C Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО в проекте ОО были подвергнуты тестированию.

Элементы действий испытательной лаборатории

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

ATE_FUN.1 Функциональное тестирование

Зависимости: ATE_COV.1 Свидетельство покрытия.

Элементы действий заявителя

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

ATE_FUN.1.2D Заявитель должен представить тестовую документацию.

Элементы содержания и представления свидетельств

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

ATE_FUN.1.2C В планах тестирования должны быть идентифицированы тесты, которые необходимо выполнить, а также должны содержаться описания сценариев проведения каждого теста. В эти сценарии должны быть включены также любые зависимости последовательности выполнения тестов от результатов других тестов.

ATE_FUN.1.3C Ожидаемые результаты тестирования должны продемонстрировать прогнозируемые данные на выходе успешного выполнения тестов.

ATE_FUN.1.4C Фактические результаты тестирования должны соответствовать ожидаемым.

Элементы действий испытательной лаборатории

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

ATE_IND.2 Выборочное независимое тестирование

Зависимости: ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации.
AGD_OPE.1 Руководство пользователя по эксплуатации.
AGD_PRE.1 Подготовительные процедуры.
ATE_COV.1 Свидетельство покрытия.
ATE_FUN.1 Функциональное тестирование.

Элементы действий заявителя

ATE_IND.2.1D Заявитель должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.2.1C ОО должен быть пригоден для тестирования.

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

Элементы действий испытательной лаборатории

ATE_IND.2.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.2.2E Испытательная лаборатория должна выполнить **все тесты** из тестовой документации, чтобы верифицировать результаты тестирования, полученные заявителем.

ATE_IND.2.3E Испытательная лаборатория должна протестировать ФБО так, чтобы подтвердить, что **все** ФБО функционируют в соответствии со спецификациями.

7.2.6. AVA: Оценка уязвимостей

AVA_VAN.4 Методический анализ уязвимостей

Зависимости: ADV_ARC.1 Описание архитектуры безопасности.
ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации.
ADV_TDS.3 Базовый модульный проект.
ADV_IMP.1 Представление реализации ФБО.
AGD_OPE.1 Руководство пользователя по эксплуатации.
AGD_PRE.1 Подготовительные процедуры

Элементы действий заявителя

AVA_VAN.4.1D Заявитель должен **выполнить анализ уязвимостей ОО**.

Элементы содержания и представления свидетельств

AVA_VAN.4.1C **Документация анализа уязвимостей должна:**
содержать результаты анализа, выполненного для поиска способов, которыми потенциально может быть нарушена реализация ФТБ;
идентифицировать проанализированные предполагаемые уязвимости;
демонстрировать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

Элементы действий испытательной лаборатории

AVA_VAN.4.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VAN.4.2E Испытательная лаборатория должна выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA_VAN.4.3E Испытательная лаборатория должна провести независимый методический анализ уязвимостей ОО с использованием документации руководств, функциональной спецификации, проекта ОО, описания архитектуры безопасности и представления реализации, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA_VAN.4.4E Испытательная лаборатория должна провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим Умеренным потенциалом нападения.

7.2.7. 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.

7.3. Обоснование требований безопасности

7.3.1. Обоснование требований безопасности для объекта оценки

7.3.1.1. Обоснование функциональных требований безопасности объекта оценки

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

Таблица 7.3. - 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**
FAU_SAR.1						**X**
FAU_SAR.3						**X**
FDP_IFC_EXT.3					**X**	
FDP_IFF_EXT.7				**X**	**X**	
FMT_SMF.1	**X**	**X**	**X**			
FMT_MOF.1	**X**	**X**				
FMT_MTD.1	**X**		**X**			
FMT_SMR.1	**X**					
FPT_ITT.1					**X**	

Включение указанных в таблице 7.3 функциональных требований безопасности ОО в ПЗ определяется документом «Требования к средствам контроля съемных машинных носителей информации», утвержденным приказом ФСТЭК России от 28 июля 2014 г. № 87.

FAU_ARP.1 Сигналы нарушения безопасности

Выполнение требований данного компонента способствует обнаружению попыток нарушения безопасности и обеспечивает функцию оповещения об этом администратора СКН. 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.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность прочтения информации аудита, которая для уполномоченных пользователей является понятной. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает возможность выполнения сортировки данных аудита, основываясь на определенных атрибутах. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации

Выполнение требований данного компонента обеспечивает управление подключаемых съемных машинных носителей. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации

Выполнение требований данного компонента обеспечивает управление подключаемыми съемными машинными носителями информации в части контроля интерфейсов ввода (вывода), к которым осуществляется подключение, контроля типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-4, Цель безопасности-5** и способствует их 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

Выполнение требований данного компонента обеспечивает разрешение ФБО на модификацию режима выполнения функций СКН администраторам СКН и другим уполномоченным ролям. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2** и способствует их достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность со стороны администраторов СКН управлять данными (данными СКН), используемыми функциями безопасности СКН. 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_ITT.1 Базовая защита внутренней передачи данных функций безопасности средства контроля съемных машинных носителей информации

Выполнение требований данного компонента обеспечивает возможность защиты данных СКН от модификации при передаче между ПО управления СКН и ПО взаимодействия СКН и подключаемых съемных машинных носителей информации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

7.3.1.2. Обоснование удовлетворения зависимостей функциональных требований безопасности

В таблице 7.4 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 7.4 является справочным и содержит компоненты, определенные в ГОСТ Р ИСО/МЭК 15408–2 в описании компонентов требований, приведенных в столбце 1 таблицы 7.4, под рубрикой «Зависимости».

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

Таблица 7.4. - Зависимости функциональных требований безопасности

Функциональный компонент	**Зависимость в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 6.1 настоящего ПЗ**	**Удовлетворение зависимости**
FAU_ARP.1	FAU_SAA.1	Цель для среды функционирования ОО-4
FAU_GEN.1	FPT_STM.1	Цель для среды функционирования ОО-4
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1

Окончание таблицы 7.4.

Функциональный компонент	Зависимость в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 6.1 настоящего ПЗ	Удовлетворение зависимости
FAU_SAR.3	FAU_SAR.1	FAU_SAR.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_MTD.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.

7.3.2. Обоснование требований доверия к безопасности объекта оценки

Требования доверия настоящего ПЗ соответствуют ОУДЗ, усиленному компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ADV_FSP.4 «Полная функциональная спецификация», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей» и расширенному компонентом AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства контроля съемных машинных носителей информации».

Включение указанных требований доверия к безопасности ОО в ПЗ определяется документом «Требования к средствам контроля съемных машинных носителей информации», утвержденным приказом ФСТЭК России от 28 июля 2014 г. № 87.