Утвержден ФСТЭК России
6 марта 2012 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ ФСТЭК РОССИИ

ПРОФИЛЬ ЗАЩИТЫ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ УРОВНЯ СЕТИ ШЕСТОГО КЛАССА ЗАЩИТЫ

ИТ.СОВ.С6.ПЗ

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место

БРП – база решающих правил

ЗБ – задание по безопасности

ИС – информационная система

ИТ – информационная технология

ОДФ – область действия функции безопасности

ОО – объект оценки

ОУД – оценочный уровень доверия

ПБО – политика безопасности объекта оценки

ПЗ – профиль защиты

СОВ – система обнаружения вторжений

УК – управление конфигурацией

ФБО – функции безопасности объекта оценки

ФТБ – функциональные требования безопасности

1 Общие положения

Настоящий методический документ ФСТЭК России разработан и утвержден в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и предназначен для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации (далее – разработчики), заявителей на осуществление сертификации продукции (далее – заявители), а также испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям по безопасности информации (далее – оценщики) при проведении ими работ по сертификации систем обнаружения вторжений (СОВ) на соответствие Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011 г. № 638.

Настоящий методический документ ФСТЭК России детализирует и определяет взаимосвязи требований к функциям безопасности систем обнаружения вторжений, установленным Требованиями к системам обнаружения вторжений, утвержденными приказом ФСТЭК России от 6 декабря 2011 г. № 638.

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

1.1 Введение профиля защиты

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

1.2 Идентификация профиля защиты

Название ПЗ:	Профиль защиты систем обнаружения вторжений уровня сети шестого класса.
Тип СОВ:	СОВ уровня сети.
Класс защиты:	Шестой.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.СОВ.С5.ПЗ.
Идентификация ОО:	Системы обнаружения вторжений уровня сети.
Уровень доверия:	Оценочный уровень доверия 1 (ОУД1), усиленный компонентом AVA_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенный компонентами ALC_UPI_EXT.1 «Процедуры обновления базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО».
Идентификация:	Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
Ключевые слова:	Система обнаружения вторжений, ОУД1.

1.3 Аннотация профиля защиты

Настоящий ПЗ определяет требования безопасности для систем обнаружения вторжений уровня сети (объекта оценки), предназначенных для использования в информационных системах, функционирующих на базе вычислительных сетей.

Объект оценки представляет собой элемент системы защиты информации информационных систем, функционирующих на базе вычислительных сетей, и применяется совместно с другими средствами защиты информации от несанкционированного доступа к информации в информационных системах.

Объект оценки должен обеспечивать обнаружение и (или) блокирование следующих основных угроз безопасности информации, относящихся к вторжениям (атакам):

преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;

преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Основными компонентами системы обнаружения вторжений (СОВ) являются датчики (сенсоры) и анализаторы.

Датчики (сенсоры) собирают информацию о пакетах данных, передаваемых в пределах информационной системы (ИС) (сегмента ИС), в которой (котором) установлены эти датчики. Датчики СОВ уровня сети могут быть реализованы в виде программного обеспечения (ПО), устанавливаемого на стандартные программно-технические платформы, а также в виде программно-технических устройств, подключаемых к ИС (сегменту ИС). Анализаторы выполняют анализ собранной датчиками информации, генерируют отчеты по результатам анализа и управляют процессами реагирования на выявленные вторжения.

Решение об обнаружении вторжения СОВ принимают в соответствии с результатами анализа информации, собираемой датчиками СОВ, с применением базы решающих правил СОВ.

В системе обнаружения вторжений должны быть реализованы следующие функции безопасности системы обнаружения вторжений:

разграничение доступа к управлению системой обнаружения вторжений;

управление работой системы обнаружения вторжений;

управление параметрами системы обнаружения вторжений;

управление установкой обновлений (актуализации) базы решающих правил системы обнаружения вторжений;

анализ данных системы обнаружения вторжений;

аудит безопасности системы обнаружения вторжений;

сбор данных о событиях и активности в контролируемой информационной системе;

реагирование системы обнаружения вторжений.

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

обеспечение доверенного маршрута;

обеспечение доверенного канала;

обеспечение условий безопасного функционирования;

управление атрибутами безопасности.

Функции безопасности системы обнаружения вторжений должны обладать составом функциональных возможностей, обеспечивающих реализацию этих функций.

В ПЗ изложены следующие виды требований безопасности, предъявляемые к СОВ:

функциональные требования безопасности;

требования доверия к безопасности.

Функциональные требования безопасности СОВ, изложенные в ПЗ, включают:

требования по осуществлению сбора данных СОВ;

требования к анализу данных СОВ;

требования к реагированию СОВ;

требования к средствам обновления базы решающих правил СОВ;

требования по защите СОВ;

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

требования по управлению данными функций безопасности (данными СОВ);

требования по управлению ролями субъектов;

требования к средствам администрирования СОВ;

требования к аудиту функционирования СОВ.

Функциональные требования безопасности для СОВ выражены на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408-2, при этом часть требований сформулированы в явном виде в стиле компонентов из ГОСТ Р ИСО/МЭК 15408-2.

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

возможность сбора информации о сетевом трафике;

возможность выполнения анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;

возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;

возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;

возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;

уведомление администратора СОВ об обнаруженных вторжениях по отношению к контролируемым узлам ИС и нарушениях безопасности с помощью визуального отображения соответствующего сообщения на консоли управления;

возможность автоматизированного обновления базы решающих правил;

возможность со стороны уполномоченных администраторов (ролей) управлять режимом выполнения функций безопасности СОВ;

возможность со стороны уполномоченных администраторов (ролей) управлять данными СОВ;

поддержка определенных ролей для СОВ и их ассоциации с конкретными администраторами СОВ и пользователями ИС;

возможность администрирования СОВ;

возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;

возможность предоставлять возможность читать информацию из записей аудита.

Требования доверия к безопасности СОВ, изложенные в ПЗ, охватывают следующие вопросы:

управление конфигурацией;

поставка и эксплуатация;

разработка;

руководства;

поддержка жизненного цикла;

тестирование;

оценка уязвимостей;

обновление базы решающих правил.

Требования доверия к безопасности СОВ сформированы на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408–3; при этом часть требований сформулированы в явном виде в стиле компонентов из ГОСТ Р ИСО/МЭК 15408–3.

Требования доверия к безопасности СОВ образуют оценочный уровень доверия 1 (ОУД1), усиленный компонентом AVA_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенный компонентами ALC_UPI_EXT.1 «Процедуры обновления базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО».

В целях обеспечения условий для безопасного функционирования СОВ в настоящем ПЗ определены цели и требования для среды функционирования СОВ.

1.4 Соглашения

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

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

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

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

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

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

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

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

Настоящий профиль защиты содержит ряд незавершенных операций над компонентами функциональных требований безопасности. Эти операции должны быть завершены в задании по безопасности на конкретную реализацию СОВ.

1.5 Термины и определения

В настоящем ПЗ применяются следующие термины с соответствующими определениями.

Администратор СОВ – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию ОО (СОВ).

Анализатор СОВ – программный или программно-технический компонент СОВ, предназначенный для сбора информации от сенсоров (датчиков) СОВ, ее итогового анализа на предмет обнаружения вторжения (атаки) на контролируемую ИС.

База решающих правил - составная часть СОВ, содержащая информацию о вторжениях (сигнатуры), на основе которой СОВ принимает решение о наличии вторжения (атаки).

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам.

Данные СОВ – данные, собранные или созданные СОВ в результате выполнения своих функций.

Датчик (сенсор) СОВ – программный или программно-технический компонент СОВ, предназначенный для сбора и первичного анализа информации (данных) о событиях в контролируемой ИС, а также – передачи этой информации (данных) анализатору СОВ.

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

Объект оценки – подлежащая сертификации (оценке) СОВ уровня сети с руководствами по эксплуатации.

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

Профиль защиты – совокупность требований безопасности для СОВ уровня сети.

Сигнатура – характерные признаки вторжения (атаки), используемые для его (ее) обнаружения.

Система обнаружения вторжений – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

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

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

1.6 Организация профиля защиты

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

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

Раздел 3 «Среда безопасности объекта оценки» содержит описание аспектов среды безопасности ОО. В данном разделе определяется совокупность угроз, имеющих отношение к безопасному функционированию ОО, политика безопасности организации, которой должен следовать ОО, и предположения (обязательные условия) безопасного использования ОО.

В разделе 4 «Цели безопасности» определена совокупность целей безопасности для ОО и среды функционирования ОО.

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

В Разделе 6 «Обоснование» демонстрируется, что ПЗ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает идентифицированные аспекты среды безопасности ОО.

2 Описание объекта оценки

2.1 Тип изделия информационных технологий

Объектом оценки в настоящем ПЗ является система обнаружения вторжений уровня сети.

Объект оценки представляет собой программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

2.2 Основные функциональные возможности объекта оценки

В данном подразделе представлено краткое описание функциональных возможностей ОО.

Системы обнаружения вторжений, соответствующие настоящему ПЗ, должны обеспечивать:

возможность сбора информации о сетевом трафике;

возможность выполнения анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;

возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;

возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;

возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;

уведомление администратора СОВ об обнаруженных вторжениях по отношению к контролируемым узлам ИС и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления;

возможность автоматизированного обновления базы решающих правил;

возможность со стороны уполномоченных администраторов (ролей) управлять режимом выполнения функций безопасности СОВ;

возможность со стороны уполномоченных администраторов (ролей) управлять данными СОВ;

поддержка определенных ролей для СОВ и их ассоциации с конкретными администраторами СОВ и пользователями ИС;

возможность администрирования СОВ;

возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;

возможность предоставлять возможность читать информацию из записей аудита.

В общем виде архитектура СОВ включает следующие компоненты:

датчики (сенсоры) СОВ, предназначенные для сбора необходимой информации о функционировании ИС;

анализаторы СОВ, выполняющие анализ данных, собранных датчиками, с целью обнаружения вторжений;

хранилище, обеспечивающее хранение информации о событиях, зафиксированных вторжениях, а также сигнатуры вторжений и другую информацию базы решающих правил, на основании которой принимается решение о наличии вторжения;

консоль управления компонентами СОВ, позволяющая администратору безопасности конфигурировать СОВ, наблюдать за состоянием защищаемой ИС и СОВ, просматривать выявленные анализатором инциденты.

Основными компонентами СОВ являются датчик(и) и анализатор(ы) СОВ. Датчики собирают информацию о трафике, поступающем в ИС (сегменты ИС), осуществляют первичный анализ и направляют эту информацию (данные) анализатору. Анализатор выполняет анализ собранных данных, уведомляют администраторов СОВ об обнаруженных вторжениях, выполняют другие действия по реагированию, генерируют отчеты на основе собранной информации (данных).

Датчики уровня сети могут устанавливаться в разрыв канала связи контролируемого сегмента ИС; путем подключения к портам сетевого оборудования ИС, а также быть интегрированными в межсетевые экраны или в коммуникационное оборудование ИС.

Анализатор должен обладать следующими функциональными возможностями:

принимать данные от датчиков;

обрабатывать данные с целью выявления вторжений;

реагировать на выявленные вторжения. Реагирование может включать создание отчетов, отображение сообщения на консоли управления и иные возможности по реагированию.

Решение об обнаружении вторжения СОВ принимает в соответствии с результатами анализа информации, собираемой сенсорами СОВ, с применением базы решающих правил СОВ.

Администрирование ОО может выполняться удаленным или локальным способами. Локальное администрирование осуществляется непосредственно с того узла, где установлен компонент СОВ, а удаленное – посредством команд, посылаемых по каналам связи.

Кроме того, все компоненты СОВ должны обладать следующими функциональными возможностями:

осуществлять защиту (совместно с механизмами среды функционирования) собственной программной и информационной части от вмешательства;

допускать настройку своих параметров со стороны администратора безопасности;

вести журнал аудита (в том числе осуществлять регистрацию попыток изменения конфигурации, а также попыток доступа к компонентам и данным).

Типовая схема применения в ИС СОВ уровня сети представлена на рисунке 2.1.

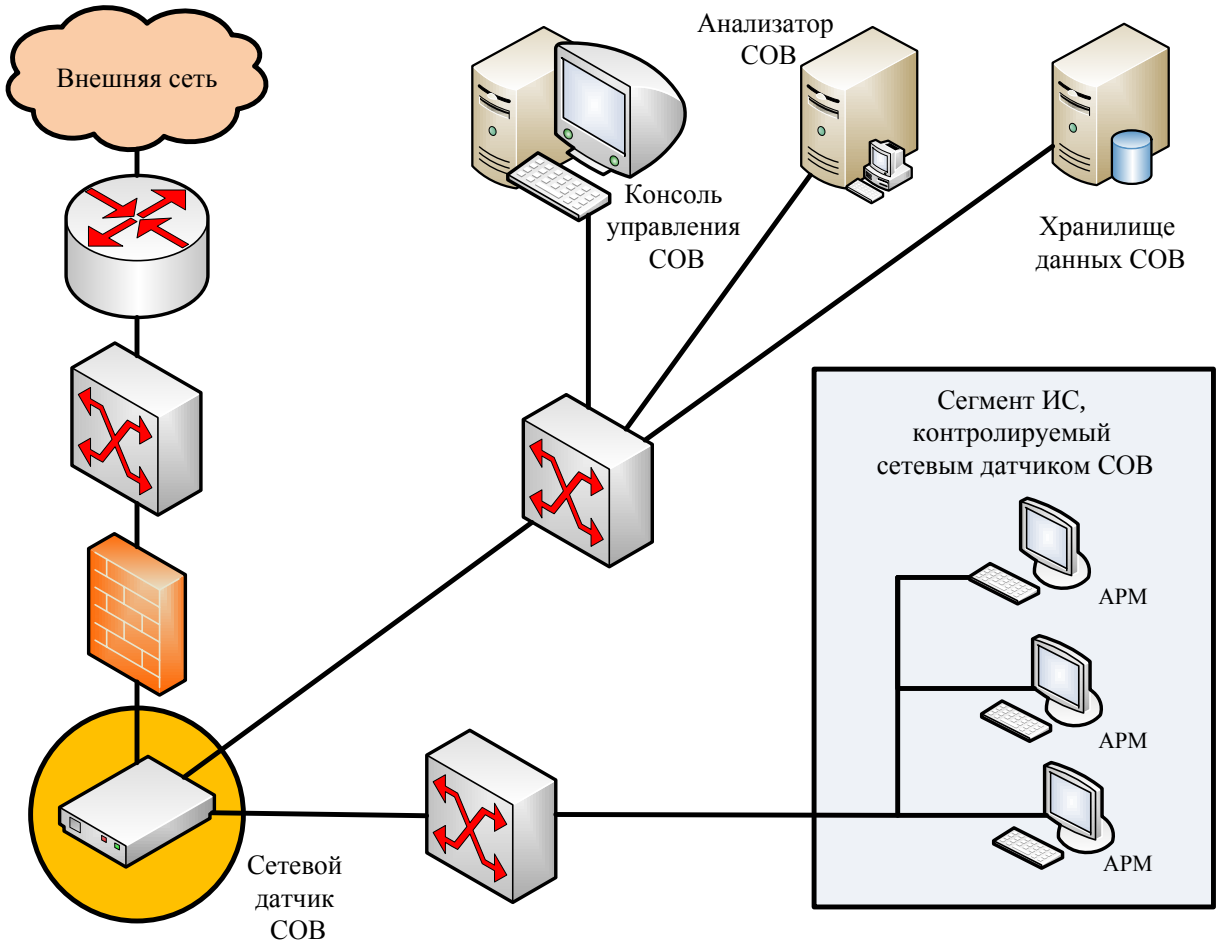

Рисунок 2.1 – Типовая схема применения в ИС СОВ уровня сети

Функционирование ОО подчинено политике безопасности ОО, отраженной в функциональных требованиях безопасности ОО.

3 Среда безопасности объекта оценки

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

предположений относительно предопределенного использования ОО и среды функционирования ОО;

угроз безопасности, которым необходимо противостоять средствами ОО;

политики безопасности организации, которой должен следовать ОО.

3.1 Предположения безопасности

Предположения относительно предопределенного использования ОО

Предположение-1

Должен быть обеспечен доступ ОО ко всем объектам ИС, которые необходимы ОО для реализации своих функциональных возможностей (к контролируемым объектам ИС).

Предположение-2

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

Предположение-3

Должна быть обеспечена совместимость ОО с элементами ИС, контроль которой он осуществляет.

Предположения, связанные с защитой ОО

Предположение-4

Должна быть обеспечена физическая защита элементов ИС, на которых установлены компоненты ОО, критически важные с точки зрения осуществления политики безопасности ОО.

Предположение-5

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

Предположение, имеющее отношение к персоналу

Предположение-6

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

3.2 Угрозы безопасности информации

3.2.1 Угрозы, которым должен противостоять объект оценки

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

Угроза-1

1. Аннотация угрозы – преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена.

2. Источник угрозы – внешние нарушители.

3. Способ реализации угрозы – обход механизмов безопасности ИС с использованием штатных средств, предоставляемых ИС, а также специализированных инструментальных средств.

4. Используемые уязвимости – недостатки средств защиты информации, применяемых в ИС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – данные пользователей, конфигурационные данные, другие ресурсы ИС.

6. Нарушаемое свойство безопасности информационных ресурсов – целостность, доступность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушения режимов функционирования ИС, снижение уровня защиты ИС.

Угроза-2

1. Аннотация угрозы – преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

2. Источник угрозы – внутренние нарушители.

3. Способ реализации угрозы – обход механизмов безопасности ИС с использованием штатных средств, предоставляемых ИС, а также специализированных инструментальных средств.

4. Используемые уязвимости – недостатки средств защиты информации, применяемых в ИС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – данные пользователей, конфигурационные данные, другие ресурсы ИС.

6. Нарушаемое свойство безопасности информационных ресурсов – целостность, доступность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушения режимов функционирования ИС, снижение уровня защиты ИС.

3.2.2 Угрозы, которым должна противостоять среда

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

Угроза среды-1

1. Аннотация угрозы – нарушение целостности данных, собранных или созданных СОВ (данных СОВ).

2. Источник угрозы – внутренний нарушитель, внешний нарушитель.

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

4. Используемая уязвимость – недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования ИС; недостатки механизмов защиты журналов аудита СОВ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – данные СОВ.

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

7. Возможные последствия реализации угрозы – невозможность использования собранной СОВ информации о возможных вторжениях (атаках) для принятия решений о реагировании.

Угроза среды-2

1. Аннотация угрозы – отключение или блокирование нарушителем компонентов СОВ.

2. Источник угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированный доступ к компонентам СОВ.

4. Используемая уязвимость – недостатки процедур разграничения полномочий в ИС, уязвимости СОВ, внесенные на этапах проектирования и разработки, недостатки контроля программной среды ИС.

5. Вид информационных ресурсов, потенциально подверженные угрозе – программное обеспечение и база решающих правил СОВ.

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

7. Возможные последствия реализации угрозы – нарушение режимов функционирования СОВ, необнаружение реализуемых по отношению к ИС вторжений (атак).

Угроза среды-3

1. Аннотация угрозы – несанкционированное изменение конфигурации СОВ.

2. Источник угрозы – внутренний нарушитель, внешний нарушитель.

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

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

5. Вид информационных ресурсов, потенциально подверженные угрозе – настройки программного обеспечения СОВ.

6. Нарушаемые характеристики безопасности активов – целостность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования СОВ, необнаружение реализуемых по отношению к ИС вторжений (атак).

Угроза среды-4

1. Аннотация угрозы – несанкционированное внесение изменений в логику функционирования СОВ через механизм обновления базы решающих правил.

2. Источник угрозы – внутренние нарушители, внешние нарушители.

3. Способ реализации угрозы – осуществление несанкционированных действий с использованием штатных средств, предоставляемых ИС, а также специализированных инструментальных средств.

4. Используемая уязвимость – недостатки механизмов обеспечения доверенного канала получения обновлений базы решающих правил СОВ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – программное обеспечение и база решающих правил СОВ.

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

7. Возможные последствия реализации угрозы – нарушение режимов функционирования СОВ, необнаружение реализуемых по отношению к ИС вторжений (атак), невозможность использования собранной СОВ информации о возможных вторжениях (атаках) для принятия решений о реагировании.

3.3 Политика безопасности организации

Объект оценки должен следовать приведенным ниже правилам политики безопасности организации.

Политика безопасности-1

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

Политика безопасности-2

Объект оценки должен осуществлять сбор информации о сетевом трафике.

Политика безопасности-3

Должна осуществляться аналитическая обработка собранных СОВ данных о функционировании контролируемой ИС заданными методами с целью вынесения решения об обнаружении вторжения.

Политика безопасности-4

Должно осуществляться реагирование СОВ на выявленные вторжения.

Политика безопасности-5

Должно осуществляться управление со стороны уполномоченных администраторов СОВ режимами выполнения функций безопасности СОВ.

Политика безопасности-6

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

Политика безопасности-7

Должна быть обеспечена возможность регистрации и учета выполнения функций безопасности СОВ.

Политика безопасности-8

Объект оценки должен иметь интерфейс администрирования.

Политика безопасности-9

Объект оценки должен иметь возможность управления режимами получения и установки обновлений (актуализации) базы решающих правил (БРП) СОВ.

4 Цели безопасности

4.1 Цели безопасности для объекта оценки

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Управление параметрами СОВ

Объект оценки должен обеспечить возможность управления параметрами СОВ (правилами в БРП СОВ, другими данными СОВ), которые влияют на выполнение функций безопасности СОВ, со стороны уполномоченных администраторов СОВ.

Цель безопасности-2

Сбор данных о событиях и активности в контролируемой ИС

Объект оценки должен осуществлять сбор информации о передаче сетевого трафика.

Цель безопасности-3

Анализ данных СОВ

Объект оценки должен осуществлять аналитическую обработку собранных СОВ данных о функционировании контролируемой ИС заданными методами с целью вынесения решения об обнаружении вторжения.

Цель безопасности-4

Реагирование СОВ

Объект оценки должен осуществлять реагирование на выявленные вторжения.

Цель безопасности-5

Управление работой СОВ

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

Цель безопасности-6

Разграничение доступа к управлению СОВ

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

Цель безопасности-7

Аудит безопасности СОВ

Объект оценки должен обеспечить регистрацию и учет выполнения функций безопасности СОВ.

Цель безопасности-8

Интерфейс СОВ

ОО должен предоставлять администратору СОВ интерфейс администрирования.

Цель безопасности-9

Управление установкой обновлений (актуализации) БРП СОВ

ОО должен иметь возможность управления режимами получения и установки обновлений (актуализации) БРП СОВ.

4.2 Цели безопасности для среды

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

Цель для среды функционирования ОО-1

Доступ к данным ИС

Должен быть обеспечен доступ объекта оценки ко всем объектам ИС, которые необходимы объекту оценки для реализации своих функциональных возможностей (к контролируемым объектам ИС).

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

Совместимость

Должна быть обеспечена совместимость объекта оценки с элементами ИС, контроль которой он осуществляет.

Цель для среды функционирования ОО-4

Физическая защита частей ОО

Должна быть обеспечена физическая защита элементов ИС, на которых установлены компоненты ОО, критически важные с точки зрения осуществления политики безопасности ОО.

Цель для среды функционирования ОО-5

Доверенная связь

Должна быть обеспечена доверенная связь (маршрут) между СОВ и администраторами СОВ.

Цель для среды функционирования ОО-6

Механизмы аутентификации и идентификации

Функционирование ОО должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов СОВ.

Цель для среды функционирования ОО-7

Доверенный канал

Должен быть обеспечен доверенный канал получения обновлений БРП СОВ.

Цель для среды функционирования ОО-8

Защита данных функций безопасности объекта оценки (ФБО)

Должна быть обеспечена защищенная область для выполнения функций безопасности СОВ.

Цель для среды функционирования ОО-9

Синхронизация по времени

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

Цель для среды функционирования ОО-10

Хранение данных аудита

Должны быть обеспечены защита журнала аудита от несанкционированного изменения и удаления, а также возможность управления событиями, потенциально приводящими к переполнению областей хранения данных аудита.

Цель для среды функционирования ОО-11

Управление атрибутами безопасности

Возможность управления атрибутами безопасности компонентов СОВ и контролируемых объектов ИС должна предоставляться только уполномоченным ролям (администраторов СОВ и ИС).

Цель для среды функционирования ОО-12

Требования к персоналу

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

5 Требования безопасности

В данном разделе ПЗ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из ГОСТ Р ИСО/МЭК 15408–2. 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, усиленного компонентом AVA_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенного компонентами ALC_UPI_EXT.1 «Процедуры обновления базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО». Требования безопасности ALC_UPI_EXT.1 «Обновление базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО» сформулированы в явном виде (расширение ГОСТ Р ИСО/МЭК 15408–3).

5.1 Требования безопасности для объекта оценки

5.1.1 Функциональные требования безопасности ОО

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

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО.

Компонент	Название компонента
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MTD.1	Управление данными ФБО
FMT_SMR.1	Роли безопасности
FID_COL_EXT.1	Сбор данных о сетевом трафике
FID_ANL_EXT.1	Базовый анализ данных СОВ
FID_MTH_EXT.1	Методы анализа
FID_MTH_EXT.2	Детализация эвристического метода анализа
FID_RCT_EXT.1	Базовое реагирование СОВ
FID_PCL_EXT.1	Анализ протоколов

Компонент	Название компонента
FID_CON_EXT.1	Механизмы администрирования
FID_UPD_EXT.1	Обновление БРП СОВ
FID_INF_EXT.1	Интерфейс СОВ

5.1.1.1 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 [выбор (выбрать одно из): *минимальный, базовый, детализированный, неопределенный*] уровне аудита;

в) [события, приведенные во втором столбце таблицы 5.2].

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

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

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ/ЗБ, [информацию, определенную в третьем столбце таблицы 5.2].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Дополнительно регистрируемая информация
FAU_GEN.1	Запуск и завершение выполнения функций аудита. Доступ к ОО	Идентификатор объекта, вид запрашиваемого доступа
FAU_SAR.1	Чтение информации из записей аудита	
FMT_MOF.1	Все модификации режима выполнения функций, связанных со сбором данных о системе ИТ, их анализом и ответными реакциями	
FMT_MTD.1	Все модификации данных СОВ, данных аудита и всех прочих данных ОО	

Компонент	Событие	Дополнительно регистрируемая информация
FMT_SMR.1	Модификация группы пользователей – исполнителей роли	Идентификатор пользователя
FPT_STM.1	Изменения внутреннего представления времени	

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять

[а) администратору безопасности;

б) [назначение: *уполномоченные пользователи*]]

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».

5.1.1.2 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны предоставлять возможность *модифицировать режим выполнения* **функций, связанных**

[а) со сбором данных о системе ИТ, их анализом и ответными реакциями;

б) с внутренним представлением времени],

только [администраторам безопасности].

Зависимости: FMT_SMR.1 «Роли безопасности».

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

[а) уполномоченным администраторам безопасности;

б) [назначение: *уполномоченные идентифицированные роли*]].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[а) администратор безопасности СОВ;

б) [назначение: *другие роли*]].

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

Зависимости: FIA_UID.1 «Выбор момента идентификации».

5.1.1.3 Сбор системных данных СОВ (FID_COL_EXT)

FID_COL_EXT.1 Сбор данных о сетевом трафике

FID_COL_EXT.1.1 ФБО должны быть способны собирать информацию о сетевом трафике [выбор: *сетевой адрес, используемый порт, значения полей сетевого пакета, аппаратный адрес устройства, идентификаторы протоколов, последовательность команд протоколов, размер полей пакета, интенсивность трафика и [назначение: другая информация]*].

FID_COL_EXT.1.2 ФБО должны регистрировать следующую информацию, связанную с сетевым трафиком: дату и время события, тип события, идентификатор субъекта и [назначение: *другая информация*].

Зависимости: отсутствуют.

5.1.1.4 Анализ данных СОВ (FID_ANL_EXT)

FID_ANL_EXT.1 Базовый анализ данных СОВ

FID_ANL_EXT.1.1 ФБО должны выполнять анализ собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени.

FID_ANL_EXT.1.2 По результатам анализа ФБО должны фиксировать следующую информацию:

а) дата и время, результат анализа, тип данных, идентификатор источника данных;

б) протокол (механизм), используемый для проведения вторжения;

в) [назначение: *другую информацию*].

Зависимости: отсутствуют.

5.1.1.5 Методы анализа СОВ (FID_MTH_EXT)

FID_MTH_EXT.1 Методы анализа

FID_MTH_EXT.1.1 ФБО должны выполнять анализ собранных данных с целью обнаружения вторжений с использованием *сигнатурных методов, эвристических методов* и [назначение: *другие методы*].

Зависимости: отсутствуют.

FID_MTH_EXT.2 Детализация эвристического метода анализа

FID_MTH_EXT.2.1 ФБО должны выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на *методах выявления аномалий сетевого трафика* [назначение: *другие методы*].

FID_MTH_EXT.2.2 ФБО должны выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов на уровне [назначение: *уровень эвристического анализа*].

Зависимости: отсутствуют.

5.1.1.6 Реагирование СОВ (FID_RCT_EXT)

FID_RCT_EXT.1 Базовое реагирование СОВ

FID_RCT_EXT.1.1 В случае обнаружения вторжений и нарушений безопасности, ФБО должны предпринять следующие действия:

- *осуществить фиксацию факта обнаружения вторжений или нарушений безопасности в журналах аудита;*
- *уведомить администратора безопасности об обнаруженных вторжениях и нарушениях безопасности с помощью [визуального отображения соответствующего сообщения на консоли управления] и* [назначение: *другие способы сигнализации*]

и [назначение: *список действий*].

Зависимости: отсутствуют.

5.1.1.7 Анализ протоколов (FID_PCL_EXT)

FID_PCL_EXT.1 Анализ протоколов

FID_PCL_EXT.1.1 ФБО должны иметь механизмы обнаружения вторжений на основе анализа служебной информации протоколов *сетевого уровня базовой эталонной модели взаимосвязи открытых систем* и [назначение: *другие уровни базовой эталонной модели взаимосвязи открытых систем*].

Зависимости: отсутствуют.

5.1.1.8 Управление СОВ (FID_CON_EXT)

FID_CON_EXT.1 Механизмы администрирования

FID_CON_EXT.1.1 ФБО должны иметь механизмы *локального администрирования СОВ* и [назначение: *другие механизмы администрирования*].

Зависимости: отсутствуют.

5.1.1.9 Обновление БРП СОВ (FID_UPD_EXT)

FID_UPD_EXT.1 Обновление БРП СОВ

FID_UPD_EXT.1.1 ФБО должны иметь средства автоматизированного обновления базы решающих правил.

FID_UPD_EXT.1.2 ФБО должны предоставлять возможность обновления базы решающих правил только [назначение: *идентифицированные уполномоченные роли*].

Зависимости: FMT_SMR.1.

5.1.1.10 Интерфейс СОВ (FID_INF_EXT)

FID_INF_EXT.1 Интерфейс СОВ

FID_INF_EXT.1.1 ФБО должны иметь тип интерфейса администрирования

[выбор:

а) «командная строка»;

б) графический интерфейс;

в) [назначение: *другие типы интерфейсов*]].

Зависимости: отсутствуют.

5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из ГОСТ Р ИСО/МЭК 15408–3 и образуют ОУД1, усиленный компонентом AVA_SOF.1 «Оценка стойкости функций безопасности ОО» и расширенный компонентами ALC_UPI_EXT.1 «Процедуры обновления базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО» (см. таблицу 5.3).

Таблица 5.3 – Требования доверия к безопасности ОО

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

5.1.2.1 Управление конфигурацией (ACM)

ACM_CAP.1 Номера версий

Зависимости отсутствуют.

Элементы действий разработчика

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

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

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

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

5.1.2.2 Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Зависимости

AGD_ADM.1 Руководство администратора.

Элементы действий разработчика

ADO_IGS.1.1D Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

Элементы содержания и представления свидетельств

ADO_IGS.1.1C Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.

Элементы действий оценщика

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

ADO_IGS.1.2E Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

5.1.2.3 Разработка (ADV)

ADV_FSP.1 Неформальная функциональная спецификация

Зависимости

ADV_RCR.1 Неформальная демонстрация соответствия.

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

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

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

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

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

ADV_RCR.1 Неформальная демонстрация соответствия

Зависимости отсутствуют.

Элементы действий разработчика

ADV_RCR.1.1D Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

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

5.1.2.4 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация.

Элементы действий разработчика

AGD_ADM.1.1D Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования.

Элементы содержания и представления свидетельств

AGD_ADM.1.1C Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.

AGD_ADM.1.2C Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.

AGD_ADM.1.3C Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_ADM.1.4C Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.

AGD_ADM.1.5C Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.

AGD_ADM.1.6C Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.

AGD_ADM.1.7C Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_ADM.1.8C Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.

Элементы действий оценщика

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

AGD_USR.1 Руководство пользователя

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация.

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

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

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

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

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

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

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

Элементы действий оценщика

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

5.1.2.5 Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ATE_FUN.1 Функциональное тестирование.

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

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

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

5.1.2.6 Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ADV_HLD.1 Описательный проект верхнего уровня.

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

Элементы действий оценщика

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

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

5.1.2.7 Требования к ОО, сформулированные в явном виде

ALC_UPI_EXT.1 Процедуры обновления базы решающих правил

Зависимости отсутствуют.

Элементы действий разработчика

ALC_UPI_EXT.1.1D Разработчик должен разработать и реализовать процедуру фиксации момента появления нового типа вторжения, основанную на [назначение: *способы фиксации*].

ALC_UPI_EXT.1.2D Разработчик должен разработать и реализовать технологию, обеспечивающую время выпуска обновлений БРП не более [назначение: *заданное значение времени*].

ALC_UPI_EXT.1.3D Разработчик должен разработать и реализовать процедуру уведомления об обновлении БРП СОВ, основанную на [назначение: *способы уведомления*].

ALC_UPI_EXT.1.4D Разработчик должен разработать и реализовать процедуру доставки обновлений БРП СОВ, основанную на [назначение: *способы доставки обновлений*].

ALC_UPI_EXT.1.5D Разработчик должен разработать процедуру контроля целостности обновлений БРП СОВ со стороны [назначение: *идентифицированные уполномоченные роли*], основанную на [назначение: *способы контроля целостности*].

ALC_UPV_EXT.1.6D Разработчик должен разработать и реализовать процедуру представления обновлений для проведения внешнего контроля, основанную на [назначение: *способы предоставления обновлений для контроля*].

Элементы содержания и представления свидетельств

ALC_UPI_EXT.1.1C Документация процедуры фиксации момента появления нового типа вторжения должна содержать описание способов фиксации.

ALC_UPI_EXT.1.2C Свидетельство должно содержать аргументацию, что время выпуска обновлений БРП не превышает заданного.

ALC_UPI_EXT.1.3C Документация процедуры уведомления об обновлении БРП СОВ должна содержать описание способов уведомления.

ALC_UPI_EXT.1.4C Документация процедуры доставки обновлений БРП СОВ должна содержать описание способов доставки обновлений.

ALC_UPI_EXT.1.5C Документация процедуры контроля целостности обновлений БРП СОВ должна содержать описание способов контроля целостности обновлений.

ALC_UPV_EXT.1.6C Документация процедуры представления обновлений для проведения внешнего контроля должна содержать описание способов предоставления разработчиком обновлений для контроля.

Элементы действий оценщика

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

ALC_UPV_EXT.1.2E Оценщик должен проверить, что схема внешнего контроля и способы предоставления обновлений для контроля позволяют организовать и проводить их внешний контроль уполномоченной стороной.

AMA_SIA_EXT.3 Экспертиза анализа влияния обновлений базы решающих правил на безопасность системы обнаружения вторжений

Элементы действий разработчика (заявителя)

AMA_SIA_EXT.3.1D Разработчик (заявитель) должен представлять ежегодно в испытательную лабораторию материалы анализа влияния обновлений базы решающих правил на безопасность системы обнаружения вторжений и среды, в которой она функционирует, а также полный пакет обновлений базы решающих правил с момента проведения последнего внешнего контроля.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния на безопасность системы обнаружения вторжений должны для каждого обновления базы решающих правил содержать краткое описание влияния обновления на задание по безопасности, представление функций безопасности системы обнаружения вторжений, реализацию функций безопасности системы обнаружения вторжений или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.3.2C Материалы анализа влияния на безопасность системы обнаружения вторжений должны для каждого обновления базы решающих правил, влияющего на задание по безопасности, представления, реализацию функции безопасности системы обнаружения вторжений, идентифицировать все функции безопасности информационных технологий, компоненты системы обнаружения вторжений, на которые воздействует данное обновление.

AMA_SIA_EXT.3.3C Материалы анализа влияния обновлений на безопасность системы обнаружения вторжений должны для каждого обновления содержать аргументацию для принятия испытательной лабораторией решения о возможности использования обновления потребителями системы обнаружения вторжений и необходимости или отсутствии необходимости проведения повторных испытаний системы обнаружения вторжений.

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, а также то, что обновления базы решающих правил не влияют на безопасность системы обнаружения вторжений и среду ее функционирования.

5.2 Требования безопасности для среды информационных технологий

Функциями безопасности, реализуемыми средой ИТ в интересах обеспечения безопасности ОО, являются функции «Идентификация и аутентификация» и «Защита ФБО».

Функциональные компоненты из ГОСТ Р ИСО/МЭК 15408–2, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.4.

Таблица 5.4 – Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FAU_STG.2	Гарантии доступности данных аудита
FAU_STG.4	Предотвращение потери данных аудита
FIA_AFL.1	Обработка отказов аутентификации

Идентификатор компонента требований	Название компонента требований
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_AMT.1	Тестирование абстрактной машины

5.2.1 Аудит безопасности (FAU)

FAU_STG.2 Гарантии доступности данных аудита

FAU_STG.2.1 **Функции безопасности среды ИТ** должны защищать хранимые записи аудита от несанкционированного удаления.

FAU_STG.2.2 **Функции безопасности среды ИТ** должны быть способны к *выявлению* модификаций записей аудита.

FAU_STG.2.3 **Функции безопасности среды ИТ** должны обеспечить поддержку [назначение: *показатель сохранности записей аудита*] при наступлении следующих событий: [выбор: *переполнение журнала аудита, сбой, вторжение*]

Зависимости: FAU_GEN.1 «Генерация данных аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 **Функции безопасности среды ИТ** должны выполнить [выбор: *"игнорирование событий, подвергающихся аудиту", "предотвращение событий, подвергающихся аудиту, исключая предпринимаемые уполномоченным пользователем со специальными правами", "запись поверх самых старых хранимых записей аудита"*] и [генерацию предупреждения] при переполнении журнала аудита.

Зависимости: FAU_STG.2 «Защищенное хранение журнала аудита».

5.2.2 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 **Функции безопасности среды ИТ** должны обнаруживать, когда произойдет [назначение: *число попыток*] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного **в элементе FIA_AFL.1.1** числа неуспешных попыток аутентификации **функции безопасности среды ИТ** должны: [назначение: *список действий****, направленных на дальнейшее предотвращение попыток доступа со стороны субъекта, ограниченное временным интервалом***].

Зависимости: FIA_UAU.2 «Аутентификация до любых действий пользователя».

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 **Функции безопасности среды ИТ** должны предоставить механизм для верификации того, что **пароли на доступ к ОО** отвечают [назначение: *определенная метрика качества* ***паролей, включающая требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов***].

Зависимости: отсутствуют.

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 **Функции безопасности среды ИТ** должны требовать, чтобы каждый **субъект доступа к ОО** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: FIA_UID.1 «Выбор момента идентификации».

FIA_UID.2 Идентификация до любых действий пользователя

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

Зависимости: отсутствуют.

5.2.3 Защита ФБО (FPT)

FPT_RVM.1 Невозможность обхода ПБО

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

Зависимости: отсутствуют.

FPT_SEP.1 Отделение домена ФБО

FPT_SEP.1.1 **Функции безопасности среды ИТ** должны поддерживать домен безопасности для выполнения **ФБО**, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 **Функции безопасности среды ИТ** должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

FPT_AMT.1 Тестирование абстрактной машины

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

Зависимости: отсутствуют.

Замечания по применению: Представленные в данном подразделе требования могут быть реализованы средой ИТ, непосредственно ОО или совместно – средой ИТ и ОО.

6 Обоснование

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

6.1 Обоснование целей безопасности

6.1.1 Обоснование целей безопасности для ОО

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

Таблица 6.1 – Отображение целей безопасности для ОО на угрозы и политику безопасности организации.

	Цель безопасности-1	**Цель безопасности-2**	**Цель безопасности-3**	**Цель безопасности-4**	**Цель безопасности-5**	**Цель безопасности-6**	**Цель безопасности-7**	**Цель безопасности-8**	**Цель безопасности-9**
Угроза-1	X	X	X	X	X	X	X		
Угроза-2	X	X	X	X	X	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			
Политика безопасности-7							X		
Политика безопасности-8								X	
Политика безопасности-9									X

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-1**, так как обеспечивает возможность управления параметрами СОВ (правилами в БРП СОВ, другими данными СОВ), которые влияют на выполнение функций безопасности СОВ, со стороны уполномоченных администраторов СОВ.

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-2,** так как обеспечивает сбор информации о передаче сетевого трафика.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-3**, так как обеспечивает осуществление аналитической обработки собранных СОВ данных о функционировании контролируемой ИС заданными методами с целью вынесения решения об обнаружении вторжения.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-4**, так как обеспечивает осуществление реагирования на выявленные вторжения.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-5**, так как обеспечивает управление со стороны уполномоченных администраторов СОВ режимами выполнения функций безопасности СОВ.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-6**, так как обеспечивает разграничение доступа к управлению СОВ на основе ролей администраторов СОВ.

Цель безопасности-7

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности **Политика безопасности-7,** так как обеспечивает регистрацию и учет выполнения функций безопасности СОВ.

Цель безопасности-8

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-8**, так как обеспечивает наличие интерфейса администрирования.

Цель безопасности-9

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-9**, так как возможность управления режимами получения и установки обновлений (актуализации) БРП СОВ.

6.1.2 Обоснование целей безопасности для среды

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

Таблица 6.2 – Отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности организации.

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8	Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12
Предположение-1	X											
Предположение-2		X										
Предположение-3			X									
Предположение-4				X								
Предположение-5									X			
Предположение-6												X

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8	Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12
Угроза среды-1						X		X		X		
Угроза среды-2					X	X		X			X	
Угроза среды-3				X		X		X			X	
Угроза среды-4							X					

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1,** так как обеспечивает доступ объекта оценки ко всем объектам ИС, которые необходимы объекту оценки для реализации своих функциональных возможностей (к контролируемым объектам ИС).

Цель для среды функционирования ОО-2

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

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-3**, так как обеспечивает совместимость объекта оценки с элементами ИС, контроль которой он осуществляет.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-4** и противостояния угрозе для среды **Угроза для среды-3**, так как обеспечивает физическую защиту элементов ИС, на которых установлены компоненты ОО, критически важные с точки зрения осуществления политики безопасности ОО.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-2**, так как обеспечивает доверенную связь (маршрут) между СОВ и администраторами СОВ.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды **Угрозы для среды-1, 2, 3**, так как обеспечивает функционирование ОО в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов СОВ.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-4**, так как обеспечивает получение обновлений БРП СОВ по доверенному каналу.

Цель для среды функционирования ОО-8

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды **Угрозы для среды-1, 2, 3**, так как обеспечивается защищенная область для выполнения функций безопасности СОВ.

Цель для среды функционирования ОО-9

Достижение этой цели безопасности необходимо в связи с реализацией предположения **Предположение-5,** так как обеспечивается предоставление надлежащего источника меток времени и синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования.

Цель для среды функционирования ОО-10

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-1,** так как обеспечивается защита журнала аудита от несанкционированного изменения и удаления, а также возможность управления событиями, потенциально приводящими к переполнению областей хранения данных аудита.

Цель для среды функционирования ОО-11

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды **Угрозы для среды-2, 3,** так как обеспечивается предоставления возможности управления атрибутами безопасности компонентов СОВ и контролируемых объектов ИС только уполномоченным ролям (администраторов СОВ и ИС).

Цель для среды функционирования ОО-12

Достижение этой цели безопасности необходимо в связи с реализацией предположения **Предположение-5,** так как обеспечивает исполнение обязанностей персоналом, ответственным за функционирование объекта оценки, руководствуясь эксплуатационной документацией.

6.2 Обоснование требований безопасности

6.2.1 Обоснование требований безопасности для ОО

6.2.1.1 Обоснование функциональных требований безопасности ОО

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

Таблица 6.3 – Отображение функциональных требований безопасности на цели безопасности.

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9
FAU_GEN.1							X		
FAU_SAR.1							X		
FMT_MOF.1	X				X				
FMT_MTD.1	X				X				
FMT_SMR.1						X			
FID_COL_EXT.1		X							
FID_ANL_EXT.1			X						
FID_MTH_EXT.1			X						
FID_MTH_EXT.2			X						
FID_RCT_EXT.1				X					
FID_PCL_EXT.1		X							
FID_CON_EXT.1					X				
FID_UPD_EXT.1									X
FID_INF_EXT.1								X	

Включение указанных в таблице 6.3 функциональных требований безопасности ОО в ПЗ определяется нормативным правовым актом ФСТЭК России «Требования к системам обнаружения вторжений».

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-7** 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-7** и способствует ее достижению.

FMT_MOF.1 Управление режимом выполнения функций безопасности

Выполнение требований данного компонента обеспечивает, что ФБО разрешает модификацию режима выполнения функций связанных со сбором данных об ИС, их анализом и ответными реакциями только уполномоченным администраторам ОО. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность запроса и добавления данных компонентов ОО и данных аудита, запроса и модификации всех прочих данных ОО, а также внесения новых правил контроля, только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_SMR.1 Роли безопасности

Выполнение требований данного компонента обеспечивает выполнение поддержки ролей безопасности и осуществления ассоциаций пользователей с ролями. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FID_COL_EXT.1 Базовый сбор системных данных

Выполнение требований данного компонента обеспечивает сбор информации о ряде событий, связанных с указываемыми ресурсами ИС. В требованиях данного компонента выделяется информация, которая должна быть включена в записи аудита и события, которые должны подвергаться аудиту. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FID_ANL_EXT.1 Базовый анализ данных СОВ

Выполнение требований данного компонента обеспечивает выполнение функций по анализу всех полученных данных СОВ и фиксирование в результате анализа определенной информации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FID_MTH_EXT.1 Методы анализа

Выполнение требований данного компонента обеспечивает выполнение функций по анализу всех полученных данных СОВ заданными методами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FID_MTH_EXT.2 Детализация эвристических методов анализа

Выполнение требований данного компонента обеспечивает выполнение функций по анализу всех полученных данных СОВ эвристическими методами анализа на заданном уровне. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FID_RCT_EXT.1 Базовое реагирование СОВ

Выполнение требований данного компонента обеспечивает посылку сигнала предупреждения требуемому получателю и выполнение списка соответствующих действий в случае обнаружения вторжения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FID_PCL_EXT.1 Анализ протоколов

Выполнение требований данного компонента обеспечивает наличие механизма обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня модели взаимодействия открытых систем. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FID_CON_EXT.1 Механизмы администрирования

Выполнение требований данного компонента обеспечивает наличие механизмов локального администрирования. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FID_UPD_EXT.1 Обновление БРП СОВ

Выполнение требований данного компонента обеспечивает наличие средств автоматизированного обновления базы решающих правил. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-9** и способствует ее достижению.

FID_INF_EXT.1 Интерфейс СОВ

Выполнение требований данного компонента обеспечивает наличие интерфейса администрирования. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-8** и способствует ее достижению.

6.2.1.2 Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ПЗ соответствуют ОУД1, усиленному компонентом ALC_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенному компонентами ALC_UPI_EXT.1 «Процедуры обновления базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО».

Включение указанных требований доверия к безопасности ОО в ПЗ определяется нормативным правовым актом ФСТЭК России «Требования к системам обнаружения вторжений».

6.2.2 Обоснование требований безопасности для среды информационных технологий

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

Таблица 6.4 – Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	Цель для среды функционирования ОО-6	**Цель для среды функционирования ОО-8**	**Цель для среды функционирования ОО-10**
FAU_STG.2			**X**
FAU_STG.4			**X**
FIA_AFL.1	**X**		
FIA_SOS.1	**X**		
FIA_UAU.2	**X**		
FIA_UID.2	**X**		
FPT_RVM.1		**X**	
FPT_SEP.1		**X**	
FPT_AMT.1		**X**	

FAU_STG.2 Гарантии доступности данных аудита

Выполнение требований данного компонента обеспечивает защиту журнала аудита от несанкционированного изменения и удаления. При этом доступ к журналу аудита разрешен только уполномоченным на это ролям. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-10** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает уполномоченной роли возможность управления журналом аудита, когда последний становится полным. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-10** и способствует ее достижению.

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает выполнение определенных действий, направленных на дальнейшее предотвращение попыток доступа со стороны субъекта, ограниченное временным интервалом, при достижении определенного числа неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-6** и способствует ее достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает верификацию качества паролей на доступ к ОО. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-6** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа к ОО до того, как функции безопасности среды ИТ разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-6** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации **с**убъекта доступа до того, как функции безопасности среды ИТ разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-6** и способствует ее достижению.

FPT_RVM.1 Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-8** и способствует ее достижению.

FPT_SEP.1 Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-8** и способствует ее достижению.

FPT_AMT.1 Тестирование абстрактной машины

Выполнение требований данного компонента обеспечивает тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной, перед использованием компонентов ОО. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-8** и способствует ее достижению.

6.2.3 Обоснование удовлетворения зависимостей требований

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

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

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

Таблица 6.5 – Зависимости функциональных требований.

Функциональные компоненты	**Зависимости по ГОСТ Р ИСО/МЭК 15408**	**Удовлетворение зависимостей**
FAU_GEN.1	FPT_STM.1	Цель для среды функционирования-9
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FID_UPD_EXT.1	FMT_SMR.1	FMT_SMR.1

Все зависимости включенных в ПЗ компонентов ФТБ удовлетворены.