ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утверждён ФСТЭК России
12 сентября 2016 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ МЕЖСЕТЕВЫХ ЭКРАНОВ ТИПА «Г» ПЯТОГО КЛАССА ЗАЩИТЫ

ИТ.МЭ.Г5.ПЗ

2016

Содержание

Перечень сокращений

ЗБ – задание по безопасности
ИС – информационная система
ИТ – информационная технология
МЭ – межсетевой экран
ОО – объект оценки
ОУД – оценочный уровень доверия
ПЗ – профиль защиты
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
ТДБ – требования доверия к безопасности объекта оценки
УК – управление конфигурацией
ФБО – функциональные возможности безопасности объекта оценки
ФТБ – функциональные требования безопасности к объекту оценки

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, производители), заявителей на осуществление сертификации продукции (далее – заявители), а также для 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 МЭ на соответствие Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 г. № 9.

Настоящий методический документ ФСТЭК России детализирует и определяет взаимосвязи требований и функций безопасности МЭ, установленных Требованиями к межсетевым экранам, утвержденными приказом ФСТЭК России от 9 февраля 2016 г. № 9.

Профиль защиты учитывает положения комплекса национальных стандартов 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 ПЗ, которые предоставляют маркировку и описательную информацию, необходимую для контроля и идентификации ПЗ и ОО, к которому он относится. Подраздел «Аннотация объекта оценки» содержит краткое описание использования ОО и его основные характеристики безопасности.

2.1. Ссылка на профиль защиты

Наименование ПЗ:	Профиль защиты МЭ типа «Г» пятого класса защиты.
Тип МЭ:	МЭ типа «Г».
Класс защиты:	Пятый.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.МЭ.Г5.ПЗ.
Идентификация ОО:	МЭ типа «Г» пятого класса защиты.
Уровень доверия:	Оценочный уровень доверия 2 (ОУД2), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана».
Идентификация:	Требования к межсетевым экранам, утвержденные приказом ФСТЭК России от 09 февраля 2016 г. № 9. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
Ключевые слова:	Межсетевые экраны, МЭ, ОУД2.

2.2. Аннотация профиля защиты

Настоящий ПЗ определяет требования безопасности к МЭ уровня веб-сервера (тип «Г»).

2.2.1. Использование и основные характеристики безопасности объекта оценки

ОО представляет собой программное или программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков, и используемое в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа.

ОО должен обеспечивать нейтрализацию следующих угроз безопасности информации:

несанкционированный доступ к информации веб-сервера;

отказ в обслуживании сервера, обслуживающего сайты, веб-службы и веб-приложения;

несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности.

В МЭ не должно содержаться программ, не выполняющих (не задействованных в реализации) функций безопасности или не предназначенных для обеспечения функционирования межсетевого экрана (сторонних программ).

В МЭ должны быть реализованы следующие функции безопасности:

контроль и фильтрация;

идентификация и аутентификация;

регистрация событий безопасности (аудит);

обеспечение бесперебойного функционирования и восстановление;

тестирование и контроль целостности;

управление (администрирование);

взаимодействие с другими средствами защиты информации.

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

исключение каналов связи в обход правил фильтрации;

обеспечение доверенного канала;

обеспечение доверенного маршрута;

физическая защита;

обеспечение безопасного функционирования;

тестирование и контроль целостности;

обеспечение взаимодействия с сертифицированными средствами защиты информации;

контроль шифрованного потока.

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

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

функциональные требования безопасности МЭ;

требования доверия к безопасности МЭ.

Функциональные требования безопасности МЭ, изложенные в ПЗ, включают:

требования к управлению потоками информации;

требования к регистрации событий безопасности (аудиту);

требования к обеспечению бесперебойного функционирования МЭ и восстановлению;

требования к тестированию и контролю целостности ПО МЭ;

требования к управлению МЭ.

Функциональные требования безопасности для МЭ выражены на основе компонентов требований из национального стандарта 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 специальных (расширенных) компонентов.

Состав функциональных требований безопасности, включенных в настоящий ПЗ, обеспечивает следующие функциональные возможности МЭ типа «Г»:

возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций передачи контролируемой МЭ информации к веб-серверу и от веб-сервера;

возможность обеспечить, чтобы в межсетевом экране фильтрация распространялась на все операции перемещения через МЭ информации к веб-серверу и от веб-сервера;

возможность поддержки контроля и анализа запросов и ответов по протоколу передачи гипертекста определенных версий;

возможность поддержки контроля и анализа сообщений, отправляемых веб-браузером веб-серверу и содержащих текстовый контент определенных кодировок и нетекстовый контент определенных типов (изображения, аудиоинформация, видеоинформация, программы);

возможность поддержки контроля и анализа специальных маркеров взаимодействия (куки) определенных типов, отправляемых веб-сервером веб-браузеру и возвращаемых веб-браузером веб-серверу, содержащих персонифицированную информацию сеанса взаимодействия пользователя с веб-сервером, основываясь на определенных атрибутах куки;

возможность явно разрешать информационный поток, базируясь на устанавливаемом администратором МЭ наборе правил фильтрации, основанных на идентифицированных атрибутах;

возможность явно запрещать информационный поток, базируясь на устанавливаемом администратором МЭ наборе правил фильтрации, основанных на идентифицированных атрибутах;

возможность блокирования всех информационных потоков, проходящих через нефункционирующий или функционирующий некорректно МЭ;

возможность блокирования неразрешенного информационного потока по протоколу передачи гипертекста одним или несколькими способами:

блокирование запроса по протоколу передачи гипертекста;

разрыв сетевого соединения;

перезапуск сетевого соединения;

блокирование взаимодействия с конкретным сетевым адресом;

блокирование сессии на уровне конкретного приложения;

блокирование взаимодействия на уровне конкретного пользователя приложения;

отправка управляющего сигнала на иной МЭ (тип «А») для блокирования неразрешенного информационного потока;

возможность уведомления (оповещения) администратора МЭ о выполненной блокировке неразрешенного информационного потока по протоколу передачи гипертекста;

возможность отключения примененной блокировки информационных потоков администратором МЭ;

возможность поддержки виртуализации внешнего представления приложений веб-сервера на уровне трансляции сетевых портов;

возможность определения виртуализированных (видимых для веб-браузера) сетевых портов приложений и их сопоставления с реальными (видимыми для веб-сервера) сетевыми портами приложений;

возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования;

возможность тестирования (самотестирования) функций безопасности МЭ (контроль целостности исполняемого кода МЭ);

возможность регистрации и учета выполнения проверок информации сетевого трафика;

возможность читать информацию из записей аудита уполномоченным администраторам;

возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита;

возможность оповещения уполномоченных лиц о критичных видах событий безопасности, в том числе сигнализация о событиях безопасности, связанных с обнаружением неразрешенных информационных потоков по протоколу передачи гипертекста;

возможность регистрации возникновения событий, которые 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» включены в минимальный уровень аудита;

возможность аутентификации администратора МЭ до разрешения любого действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора;

возможность идентификации администратора МЭ до разрешения любого действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора;

возможность осуществления идентификации пользователя до разрешения передачи через МЭ информационного потока, ассоциированного с этим пользователем, к веб-серверу (от веб-сервера);

поддержка определенных ролей по управлению МЭ;

возможность со стороны администраторов МЭ управлять данными МЭ, используемыми функциями безопасности МЭ;

возможность со стороны администраторов МЭ управлять атрибутами безопасности;

предоставление возможности администраторам МЭ назначать, модифицировать, удалять разрешительные и (или) запретительные атрибуты для информации по протоколу передачи гипертекста для осуществления фильтрации;

возможность со стороны администраторов МЭ управлять режимом выполнения функций безопасности МЭ.

Требования доверия к безопасности МЭ сформированы на основе компонентов требований из национального стандарта Российской Федерации 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» и специальных (расширенных) компонентов.

Требования доверия к безопасности МЭ образуют оценочный уровень доверия 2 (ОУД2), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана».

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

2.2.2. Тип объекта оценки

ОО является МЭ типа «Г».

МЭ типа «Г» – это МЭ, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера). Межсетевые экраны типа «Г» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера.

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

В рамках настоящего ПЗ аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в состав объекта оценки, не рассматриваются.

2.3. Соглашения

Комплекс национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» допускает выполнение определенных операций над компонентами требова0ний безопасности. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

Операция **«уточнение»** используется для добавления в компонент требований некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей по удовлетворению требований. Результат операции **«уточнение»** в настоящем ПЗ обозначается **полужирным текстом**.

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

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

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

Операция **«итерация»** используется для выражения двух или более требований безопасности на основе одного компонента требований безопасности; при этом осуществляется различное выполнение других операций («уточнение», «выбор» и (или) «назначение») над этим компонентом.

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

3. Утверждение о соответствии

3.1. Утверждение о соответствии ГОСТ Р ИСО/МЭК 15408

Настоящий профиль защиты разработан с учетом положений национальных стандартов 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 (специальные) требования безопасности, разработанные в соответствии с правилами, установленными комплексом национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана», FDP_IFF_EXT.7 «Базовая поддержка атрибутов протокола передачи гипертекста», FFW_ARP_EXT.2 «Блокирование передачи гипертекста», FFW_EVP_EXT.1 «Виртуализация внешнего представления приложений»).

3.2. Утверждение о соответствии профилям защиты

Соответствие другим профилям защиты не требуется.

3.3. Утверждение о соответствии пакетам

Заявлено о соответствии настоящего ПЗ следующему пакету:

пакет требований доверия: оценочный уровень доверия 2 (ОУД2), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана».

3.4. Обоснование соответствия

Включение функциональных требований и требований доверия к безопасности МЭ в настоящий ПЗ определяется Требованиями к межсетевым экранам, утвержденными приказом ФСТЭК России от 9 февраля 2016 г. № 9.

3.5. 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 МЭ проблемы безопасности:

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

политики безопасности, которую должен выполнять ОО;

предположений безопасности (обязательных условий безопасного использования ОО).

4.1. Угрозы

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 – несанкционированный доступ к информации веб-сервера.

2. Источники угрозы – внешний нарушитель, внутренний нарушитель.

3. Способ реализации угрозы – установление сетевых соединений веб-сервером, не предусмотренные технологией обработки информации.

4. Используемые уязвимости – наличие неконтролируемых сетевых подключений к веб-серверу, недостатки настройки механизмов защиты информации.

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

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

7. Возможные последствия реализации угрозы – несанкционированный доступ к информационным ресурсам ИС, нарушение режимов функционирования ИС.

Угроза-2

1. Аннотация угрозы – отказ в обслуживании сервера, обслуживающего сайты, веб-службы и веб-приложения;

.

2. Источники угрозы – внешний нарушитель.

3. Способ реализации угрозы – установление не предусмотренных технологией обработки информации в информационной системе сетевых соединений с веб-сервером для отправки множества сетевых пакетов (запросов) до заполнения ими сетевой полосы пропускания канала передачи данных или отправки специально сформированных аномальных сетевых пакетов (запросов) больших размеров или нестандартной структуры.

4. Используемые уязвимости – наличие неконтролируемых сетевых подключений к веб-серверу, уязвимости сетевых протоколов, недостатки настройки механизмов защиты, уязвимости в программном обеспечении программно-аппаратных средств ИС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – пользовательские данные, сервисы информационной системы.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Возможные последствия реализации угрозы – невозможность обработки запросов уполномоченных пользователей ИС; невозможность предоставления доступа к компонентам ИС.

Угроза-3

1. Аннотация угрозы – несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – отправка специально сформированных сетевых пакетов на интерфейсы МЭ, приводящих к отключению, обходу или преодолению механизмов защиты МЭ с использованием штатных средств или специализированных инструментальных средств.

4. Используемые уязвимости – недостатки средств защиты информации, применяемых на веб-сервере; недостатки собственных защитных механизмов МЭ; недостатки настройки функциональных возможностей безопасности МЭ.

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

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

7. Возможные последствия реализации угрозы – нарушения режимов функционирования МЭ и веб-сервера.

4.1.2. Угрозы, которым противостоит среда

В настоящем ПЗ определена следующая угроза, которой должна противостоять среда функционирования ОО:

Угроза среды - 1

1. Аннотация угрозы – нарушение целостности ПО МЭ, настроек МЭ.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

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

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

5. Вид информационных ресурсов, потенциально подверженных угрозе – программное обеспечение МЭ, данные функций безопасности МЭ.

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

7. Возможные последствия реализации угрозы – нарушение режимов функционирования МЭ, неэффективность работы МЭ.

4.2. Политика безопасности

ОО должен выполнять приведенные ниже правила политики безопасности.

Политика безопасности-1

Должны обеспечиваться контроль и фильтрация информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера.

Политика безопасности-2

Должна обеспечиваться интерпретация управляющих сигналов от средств защиты информации и блокирование соответствующего трафика.

Политика безопасности-3

Должно осуществляться разграничение доступа к управлению МЭ и параметрами МЭ на основе ролей уполномоченных лиц.

Политика безопасности-4

Должна обеспечиваться возможность управления работой МЭ и параметрами МЭ со стороны администраторов МЭ.

Политика безопасности-5

Должны обеспечиваться идентификация и аутентификация администраторов МЭ.

Политика безопасности-6

Должны осуществляться механизмы регистрации о возможных нарушениях безопасности.

Политика безопасности-7

Должны обеспечиваться установка безопасного состояния ФБО или предотвращение их перехода в опасное состояние после сбоев, прерывания функционирования или перезапуска.

Политика безопасности-8

Должна осуществляться выдача предупреждающих сообщений пользователю об обнаружении возможного нарушения безопасности и предоставлять пользователю возможность осуществить определенные действия при обнаружении возможного нарушения безопасности.

Политика безопасности-9

Должны обеспечиваться возможности блокирования неразрешенного информационного потока по протоколу передачи гипертекста и отключения примененной блокировки информационных потоков.

Политика безопасности-10

Должна обеспечиваться поддержка виртуализации внешнего представления приложений веб-сервера.

4.3. Предположения безопасности

Предположение, связанное с физическими аспектами среды функционирования

Предположение-1

Должна обеспечиваться физическая защита МЭ, средства вычислительной техники, на котором он функционирует и терминалов, с которых выполняется его управление.

Предположения по отношению к аспектам связности среды функционирования

Предположение-2

Должно обеспечиваться исключение каналов связи защищаемой информационной системы с иными информационными системами в обход МЭ.

Предположение-3

Должен обеспечиваться доверенный канал передачи данных между защищаемой информационной системой и МЭ, а также между МЭ и терминалом, с которого выполняется его управление.

Предположение-4

Должен обеспечиваться доверенный маршрут между МЭ и администраторами МЭ.

Предположение-5

Должно обеспечиваться взаимодействие МЭ с сертифицированными на соответствие требованиям безопасности информации по соответствующему классу защиты средствами защиты информации (системами обнаружения вторжений, средствами антивирусной защиты и другими), от которых МЭ получает управляющие сигналы.

Предположение-6

Должны быть обеспечены совместимость компонентов МЭ с компонентами средств вычислительной техники информационной системы, а также необходимые ресурсы для выполнения функций безопасности МЭ (в том числе изоляция данных и процессов МЭ от иных данных и процессов средства вычислительной техники, на котором он функционирует).

Предположение-7

Должно быть обеспечено функционирование МЭ в среде сертифицированной на соответствие требованиям безопасности информации по соответствующему классу защиты операционной системы или в среде, защищенной путем принятия мер защиты информации, соответствующих классу защищенности информационной системы (автоматизированной системы управления), для использования в которой предназначается МЭ.

Предположение-8

Должны быть обеспечены тестирование и контроль целостности аппаратных средств, а также программного обеспечения базовой системы ввода-вывода, загрузчика и операционной системы МЭ или средства вычислительной техники, на котором он функционирует.

Предположение-9

Должны обеспечиваться контроль и фильтрация шифрованного потока.

Предположение, связанное с персоналом среды функционирования

Предположение-10

Персонал, ответственный за функционирование ОО, должен обеспечивать установку, настройку и эксплуатацию МЭ в соответствии с правилами по безопасной настройке и руководством пользователя (администратора).

5. Цели безопасности

5.1. Цели безопасности для объекта оценки

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1
Управление информационными потоками

ОО должен обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера.

Цель безопасности-2
Взаимодействие МЭ с отдельными типами средств ЗИ

ОО должен обеспечивать возможность взаимодействия с отдельными типами средств защиты информации и интерпретацию результатов их работы при осуществлении фильтрации пакетов данных и блокирования соответствующего трафика.

Цель безопасности-3
Разграничение доступа к управлению МЭ

ОО должен обеспечивать разграничение доступа к управлению МЭ и параметрами МЭ на основе ролей администраторов МЭ.

Цель безопасности-4
Управление МЭ

ОО должен обеспечивать возможность управления работой МЭ и параметрами МЭ со стороны администраторов МЭ.

Цель безопасности-5
Идентификация и аутентификация администраторов МЭ

ОО должен обеспечивать идентификацию и аутентификацию администраторов МЭ.

Цель безопасности-6
Аудит безопасности МЭ

ОО должен располагать механизмами регистрации о возможных нарушениях безопасности.

Цель безопасности-7
Обеспечение бесперебойного функционирования МЭ

ОО должен устанавливать безопасное состояние ФБО или предотвращать их переход в опасное состояние после сбоев, прерывания функционирования или перезапуска.

Цель безопасности-8

Регистрация результатов проверок информационного сетевого трафика

ОО должен осуществлять выдачу предупреждающих сообщений пользователю об обнаружении возможного нарушения безопасности и предоставлять пользователю возможность осуществить определенные действия при обнаружении возможного нарушения безопасности.

Цель безопасности-9

Блокирование неразрешенного информационного потока по протоколу передачи гипертекста

Должны обеспечиваться возможности блокирования неразрешенного информационного потока по протоколу передачи гипертекста и отключения примененной блокировки информационных потоков.

Цель безопасности-10

Поддержка виртуализации внешнего представления приложений веб-сервера

Должна обеспечиваться поддержка виртуализации внешнего представления приложений веб-сервера.

5.2. Цели безопасности для среды функционирования

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

Цель для среды функционирования ОО-1

Обеспечение доверенного канала

Должен обеспечиваться доверенный канал передачи данных между защищаемым сервером (сегментом серверов), обслуживающим сайты, веб-службы и веб-приложения, и МЭ, а также между МЭ и терминалом, с которого выполняется управление МЭ.

Цель для среды функционирования ОО-2

Обеспечение доверенного маршрута

Должен быть обеспечен доверенный маршрут между МЭ и администраторами МЭ.

Цель для среды функционирования ОО-3

Обеспечение условий безопасного функционирования

Должно обеспечиваться исключение каналов связи защищаемого сервера (сегмента серверов), обслуживающего сайты, веб-службы и веб-приложения, с информационно-телекоммуникационными сетями и информационными системами в обход МЭ.

Цель для среды функционирования ОО-4

Физическая защита ОО

Должна обеспечиваться физическая защита МЭ, средства вычислительной техники, на котором он функционирует и терминалов, с которых выполняется его управление.

Цель для среды функционирования ОО-5

Взаимодействие с доверенными продуктами информационных технологий

Должно обеспечиваться взаимодействие МЭ с сертифицированными на соответствие требованиям безопасности информации по соответствующему классу защиты средствами защиты информации (системами обнаружения вторжений, средствами антивирусной защиты и другими), от которых МЭ получает управляющие сигналы.

Цель для среды функционирования ОО-6

Эксплуатация ОО

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

Цель для среды функционирования ОО-7

Требования к персоналу

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

Цель для среды функционирования ОО-8

Поддержка аудита

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

Цель для среды функционирования ОО-9

Совместимость компонентов МЭ с компонентами средств вычислительной техники

Должны быть обеспечены совместимость компонентов МЭ с компонентами средств вычислительной техники информационной системы, а также необходимые ресурсы для выполнения функций безопасности МЭ (в том числе изоляция данных и процессов МЭ от иных данных и процессов средства вычислительной техники, на котором он функционирует).

Цель для среды функционирования ОО-10

Доверенная среда функционирования

Должно быть обеспечено функционирование МЭ в среде сертифицированной на соответствие требованиям безопасности информации по соответствующему классу защиты операционной системы или в среде, защищенной путем принятия мер защиты информации, соответствующих

классу защищенности информационной системы (автоматизированной системы управления), для использования в которой предназначается МЭ.

Цель для среды функционирования ОО-11
Тестирование и контроль целостности среды функционирования

Должны быть обеспечены тестирование и контроль целостности аппаратных средств, а также программного обеспечения базовой системы ввода-вывода, загрузчика и операционной системы МЭ или средства вычислительной техники, на котором он функционирует.

Цель для среды функционирования ОО-12
Контроль и фильтрация шифрованного потока

Должны обеспечиваться контроль и фильтрация шифрованного потока.

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.

Таблица 5.1 – Отображение целей безопасности для ОО на угрозы и политику 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	Цель безопасности-10
Угроза - 1	X									
Угроза - 2	X									
Угроза - 3			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	
Политика безопасности-10										X

Цель безопасности-1

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-2** и реализации политики безопасности **Политика безопасности-1**, так как обеспечивает контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера.

Цель безопасности-2

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-2,** так как обеспечивает возможность взаимодействия с отдельными типами средств защиты информации и интерпретацию результатов их работы при осуществлении фильтрации пакетов данных и блокирования соответствующего трафика.

Цель безопасности-3

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-3** и реализации политики безопасности **Политика безопасности-3,** так как обеспечивает возможность разграничения доступа к управлению МЭ и параметрами МЭ со стороны уполномоченных лиц.

Цель безопасности-4

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-3** и реализации политики безопасности **Политика безопасности-4,** так как обеспечивает возможность управления режимами выполнения функций безопасности МЭ и параметрами МЭ.

Цель безопасности-5

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-3** и реализации политики безопасности **Политика безопасности-5,** так как обеспечивает идентификацию и аутентификацию администраторов МЭ.

Цель безопасности-6

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-3** и реализации политики безопасности **Политика безопасности-6,** так как обеспечивает возможность регистрации событий, относящихся к возможным нарушениям безопасности.

Цель безопасности-7

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-3** и реализации политики безопасности **Политика безопасности-7,** так как обеспечивает возможность устанавливать безопасное состояние ФБО или предотвращать их переход в опасное состояние после сбоев, прерывания функционирования или перезапуска.

Цель безопасности-8

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-8**, так как обеспечивает выдачу предупреждающих сообщений пользователю об обнаружении возможного нарушения безопасности и предоставление пользователю возможности выполнения определенных действий при обнаружении возможного нарушения безопасности.

Цель безопасности-9

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-9**, так как обеспечивает блокирование неразрешенного информационного потока по протоколу передачи гипертекста и отключение примененной блокировки информационных потоков.

Цель безопасности-10

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-10**, так как обеспечивает поддержку виртуализации внешнего представления приложений веб-сервера.

6. Определение расширенных компонентов

В данном разделе ПЗ представлены расширенные компоненты для МЭ.

6.1. Определение расширенных компонентов функциональных требований безопасности объекта оценки

Для МЭ типа «Г» определены следующие компоненты функциональных требований безопасности, сформулированные в явном виде в стиле компонентов из национального стандарта 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» (расширенные (специальные) компоненты).

6.1.1. Функции управления информационными потоками (семейство FDP_IFF)

Ранжирование компонентов

FDP_IFF_EXT.7 «Базовая поддержка атрибутов протокола передачи гипертекста» содержит требования поддержки контроля и анализа запросов и ответов по протоколу передачи гипертекста определенных версий, сообщений, отправляемых веб-браузером веб-серверу и содержащих текстовый контент определенных кодировок и нетекстовый контент определенных типов (изображения, аудиоинформация, видеоинформация, программы), специальных маркеров взаимодействия (куки) определенных типов, отправляемых веб-сервером веб-браузеру и возвращаемых веб-браузером веб-серверу, содержащих персонифицированную информацию сеанса взаимодействия пользователя с веб-сервером, основываясь на определенных атрибутах куки.

FDP_IFF_EXT.8 «Расширенная поддержка атрибутов протокола передачи гипертекста» содержит требования (помимо требований из FDP_IFF_EXT.7) поддержки контроля и анализа фрагментированных запросов и ответов при доступе к веб-серверу, запросов и ответов при доступе к веб-серверу, подвергшихся сжатию.

Управление: FDP_IFF_EXT.7

Действия по управлению не предусмотрены.

Аудит: FDP_IFF_EXT.7

Если в профиль защиты и (или) задание по безопасности включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) Детализированный: специфические атрибуты безопасности, используемые при принятии решений по осуществлению информационных потоков.

FDP_IFF_EXT.7 Базовая поддержка атрибутов протокола передачи гипертекста

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FDP_IFF_EXT.7.1

Функциональные возможности безопасности МЭ должны поддерживать контроль и анализ запросов и ответов по протоколу передачи гипертекста следующих версий [назначение: *поддерживаемые версии протокола передачи гипертекста*].

FDP_IFF_EXT.7.2

Функциональные возможности безопасности МЭ должны поддерживать контроль и анализ сообщений, отправляемых веб-браузером веб-серверу и содержащих текстовый контент [назначение: *кодировки*] и нетекстовый контент [выбор: *изображения, аудиоинформацию, видеоинформацию, программы, [назначение: иные типы нетекстового контента]*].

FDP_IFF_EXT.7.3

Функциональные возможности безопасности МЭ должны поддерживать контроль и анализ куки [выбор: *временные куки, постоянные куки, сторонние куки, [назначение: иные типы куки]*], отправляемых веб-сервером веб-браузеру и возвращаемых веб-браузером веб-серверу, содержащих персонифицированную информацию сеанса взаимодействия пользователя с веб-сервером, основываясь на [выбор: *типах куки, сроке действия куки, версии куки, доменном имени веб-сервера, пути к запрашиваемому ресурсу, [назначение: иных атрибутах куки]*].

6.1.2. Действия по реагированию (семейство FFW_ARP_EXT)

Характеристика семейства

Семейство FFW_ARP_EXT определяет реакцию на обнаружение возможного нарушения безопасности.

Ранжирование компонентов

В FFW_ARP_EXT.1 «Сигналы нарушения безопасности» функциональные возможности безопасности должны осуществлять определенные действия в случае обнаружения возможного нарушения безопасности.

В FFW_ARP_EXT.2 «Блокирование передачи гипертекста» функциональные возможности безопасности должны предусматривать действия по блокированию неразрешенного информационного потока по протоколу передачи гипертекста и отключению примененной блокировки информационных потоков.

FFW_ARP_EXT.2 Блокирование передачи гипертекста

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FFW_ARP_EXT.2.1

Функциональные возможности безопасности МЭ должны блокировать неразрешенный информационный поток по протоколу передачи гипертекста путем

[выбор:

а) блокирования запроса по протоколу передачи гипертекста;

б) разрыва сетевого соединения;

в) перезапуска сетевого соединения;

г) блокирования взаимодействия с конкретным сетевым адресом;

д) блокирование сессии на уровне конкретного приложения;

е) блокирование взаимодействия на уровне конкретного пользователя приложения;

ж) отправка управляющего сигнала на иной МЭ для блокирования неразрешенного информационного потока;

з) [назначение: другой способ]**].**

FFW_ARP_EXT.2.2

Функциональные возможности безопасности МЭ должны уведомлять (оповещать) о выполненной блокировке [выбор: ***администратора МЭ, пользователя информационной системы, [назначение: иные уполномоченные роли]*****].**

FFW_ARP_EXT.2.3

Функциональные возможности безопасности МЭ должны обеспечивать возможность отключения примененной блокировки информационных потоков

[выбор:

а) по запросу [назначение: уполномоченные роли];

б) [назначение: иные условия отключения блокировки]**].**

путем

[выбор:

а) полной отмены блокировки;

б) частичной отмены блокировки [выбор: для отдельных типов запросов, [назначение: иные основания частичной отмены блокировки]]**].**

6.1.3. Виртуализация внешнего представления приложений (семейство FFW_EVP_EXT)

Характеристика семейства

Семейство FFW_EVP_EXT определяет требования по виртуализации внешнего представления приложений.

Ранжирование компонентов

В FFW_EVP_EXT.1 «Виртуализация внешнего представления приложений веб-сервера» функциональные возможности безопасности должны осуществлять поддержку виртуализации внешнего представления приложений веб-сервера.

FFW_EVP_EXT.1 Виртуализация внешнего представления приложений веб-сервера

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FFW_EVP_EXT.1.1

Функциональные возможности безопасности МЭ должны поддерживать виртуализацию внешнего представления приложений веб-сервера на уровне:

[выбор:

а) трансляции сетевых портов;

б) трансляции унифицированных идентификаторов ресурсов;

***в) [назначение: другие способы виртуализации]*]**.

6.2. Определение расширенных компонентов требований доверия к безопасности объекта оценки

Для МЭ типа «Г» определены следующие расширенные (специальные) компоненты требований доверия к безопасности: ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана», сформулированные в явном виде в стиле компонентов из национального стандарта Российской Федерации 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».

6.2.1. Реализация ОО

ADV_IMP_EXT.3 Реализация ОО

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_IMP.2 Полное отображение представления реализации ФБО

Элементы действий заявителя (разработчика, производителя)

ADV_IMP_EXT.3.1D Заявитель (разработчик, производитель) должен предоставить реализацию ОО.

ADV_IMP_EXT.3.2D Заявитель (разработчик, производитель) должен обеспечить прослеживание реализации ОО к представлению реализации ФБО.

Элементы содержания и представления документированных материалов

ADV_IMP_EXT.3.1C В документации должны быть указаны состав и значения контрольных сумм элементов реализации ПО [выбор: *загрузочные модули ПО*, [назначение: *иные типы элементов реализации ПО*]].

ADV_IMP_EXT.3.2C В прослеживании между реализацией ОО и представлением реализации должно быть продемонстрировано [выбор:

а) для аппаратной платформы – соответствие между реализацией аппаратной платформы и ее представлением реализации [выбор: *схемы аппаратных средств, представления (кода) на языке описания аппаратных средств* [назначение: *иные формы представления реализации*]];

б) для ПО – соответствие между реализацией ПО [выбор: загрузочные модули ПО, [назначение: *иные типы элементов реализации ПО*]] и их представлением реализации [выбор: *исходные тексты ПО,* [назначение: *иные формы представления реализации*]]].

Элементы действий испытательной лаборатории

ADV_IMP_EXT.3.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_IMP_EXT.3.1C и ADV_IMP_EXT.3.2C.

6.2.2. Процедуры обновления программного обеспечения межсетевого экрана

ALC_FPU_EXT.1 Процедуры обновления программного обеспечения межсетевого экрана

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_FPU_EXT.1.1D Заявитель (разработчик, производитель) должен разработать и реализовать технологию обновления МЭ для [назначение: *типы обновлений*].

ALC_FPU_EXT.1.2D Заявитель (разработчик, производитель) должен разработать и поддерживать регламент обновления программного обеспечения МЭ.

ALC_FPU_EXT.1.3D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру уведомления потребителей о выпуске обновлений МЭ, основанную на [назначение: *способы уведомления*].

ALC_FPU_EXT.1.4D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру предоставления обновлений потребителям МЭ, основанную на [назначение: *способы предоставления обновлений*].

ALC_FPU_EXT.1.5D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру представления обновлений в испытательную лабораторию для проведения внешнего контроля, основанную на [назначение: *способы предоставления обновлений для контроля*].

Элементы содержания и представления документированных материалов

ALC_FPU_EXT.1.1C Документация МЭ должна содержать описание технологии выпуска обновлений МЭ.

ALC_FPU_EXT.1.2C Документация МЭ должна содержать регламент обновления МЭ, включающий:
а) идентификацию типов выпускаемых обновлений;
б) описание процедуры уведомления потребителей о выпуске обновлений;
в) описание процедуры предоставления обновлений потребителям;
г) описание содержания эксплуатационной документации на выпускаемые обновления;
д) [назначение: *иная информация*].

ALC_FPU_EXT.1.3C Регламент обновления МЭ должен предусматривать включение в эксплуатационную документацию на выпускаемые обновление описания следующих процедур:
а) процедуры получения обновления;
б) процедуры контроля целостности обновления;
в) типовой процедуры тестирования обновления;
г) процедуры установки и применения обновления;
д) процедуры контроля установки обновления;
е) процедуры верификации (проверки) применения обновления.

ALC_FPU_EXT.1.4C Документация процедуры представления обновлений для проведения внешнего контроля должна содержать:
а) описание процедуры предоставления обновлений для внешнего контроля;
б) требования к предоставлению и содержанию методики тестирования обновления заявителем;
в) требования к оформлению и предоставлению результатов тестирования обновления заявителем;
г) [назначение: *иная информация*].

Элементы действий испытательной лаборатории

ALC_FPU_EXT.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ALC_FPU_EXT.1.1C - ALC_FPU_EXT.1.4C.

ALC_FPU_EXT.1.2E Испытательная лаборатория должна проверить, что процедура представления обновлений для проведения внешнего контроля позволяет организовать и проводить их внешний контроль.

6.2.3. Анализ влияния на безопасность (AMA_SIA)

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность межсетевого экрана

Иерархический для: нет подчиненных компонентов.

Зависимости: ALC_FPU_EXT.1 Процедуры обновления программного обеспечения межсетевого экрана.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность МЭ должны содержать краткое описание влияния обновлений на задание по безопасности, функции безопасности МЭ или содержать логическое обоснование отсутствия такого влияния.

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

Элементы действий испытательной лаборатории

AMA_SIA_EXT.3.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в AMA_SIA_EXT.3.1C, AMA_SIA_EXT.3.2C.

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

7. 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 национального стандарта 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». Кроме того, в настоящий ПЗ включено ряд требований безопасности, сформулированных в явном виде (расширение национального стандарта 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»). Требования доверия основаны на компонентах требований доверия из национального стандарта Российской Федерации 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» и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД2, усиленного компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенного компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана». Требования безопасности ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана» сформулированы в явном виде (расширение национального стандарта Российской Федерации 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»).

7.1. Функциональные требования безопасности объекта оценки

Функциональные компоненты из национального стандарта 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», на которых основаны функциональные требования безопасности ОО, а также компоненты сформулированных в

явном виде расширенных (специальных) требований приведены в таблице 7.1.

Таблица 7.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_ARP.1	Сигналы нарушения безопасности
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FAU_SEL.1	Избирательный аудит
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FDP_IFC.2	Полное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FDP_IFF_EXT.7	Базовая поддержка атрибутов протокола передачи гипертекста
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MTD.1	Управление данными функций безопасности
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
FMT_MSA.1	Управление атрибутами безопасности
FPT_RCV.1	Ручное восстановление
FPT_TST.1	Тестирование функциональных возможностей безопасности
FFW_ARP_EXT.2	Блокирование передачи гипертекста
FFW_EVP_EXT.1	Виртуализация внешнего представления приложений

7.1.1. Аудит безопасности (FAU)

FAU_ARP.1 **Сигналы нарушения безопасности**

FAU_ARP.1.1 ФБО должны предпринять [назначение: *действия по оповещению уполномоченных лиц*], **в том числе – сигнализировать о событиях безопасности, связанных с обнаружением неразрешенных информационных потоков по протоколу передачи гипертекста,** при обнаружении **критичных событий безопасности**.

Зависимости: FAU_SAA.1 Анализ потенциального нарушения.

FAU_GEN.1 **Генерация данных аудита**

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

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на *минимальном* уровне аудита;
в) [результаты выполнения проверок информации сетевого трафика];
г) [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) дату 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».

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_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к осуществлению выбора совокупности событий, подвергающихся аудиту, из совокупности событий, **в отношении которых возможно осуществление аудита (в соответствии с FAU_GEN.1),** базируясь на следующих атрибутах:
а) [выбор: *идентификатор объекта, идентификатор пользователя, идентификатор субъекта, тип события*];
б) [назначение: *список дополнительных атрибутов, на которых основана избирательность аудита*].

Зависимости: FAU_GEN.1 Генерация данных аудита;
FMT_MTD.1 Управление данными ФБО.

7.1.2. Идентификация и аутентификация (FIA)

FIA_UAU.2	**Аутентификация до любых действий пользователя**
FIA_UAU.2.1	ФБО должны требовать, чтобы **администратор МЭ** был успешно аутентифицирован до разрешения **любого действия**, выполняемого при посредничестве ФБО от имени этого **администратора МЭ**.
Зависимости:	FIA_UID.1 Выбор момента идентификации.

FIA_UID.2 (1)	**Идентификация до любых действий пользователя**
FIA_UID.2.1 (1)	ФБО должны требовать, чтобы **администратор МЭ** был успешно идентифицирован до разрешения **любого действия**, выполняемого при посредничестве ФБО от имени этого **администратора МЭ**.
Зависимости:	отсутствуют.

FIA_UID.2 (2)	**Идентификация до любых действий пользователя**
FIA_UID.2.1 (2)	ФБО должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения **передачи через МЭ информационного потока, ассоциированного с этим пользователем, к веб-серверу (от веб-сервера)**.
Зависимости:	отсутствуют.

7.1.3. Защита данных пользователя (FDP)

FDP_IFC.2 (1)	**Полное управление информационными потоками**
FDP_IFC.2.1(1)	ФБО должны осуществлять [фильтрацию] для [отправители информации, получатели информации, сетевой трафик] и всех операций перемещения **контролируемой МЭ** информации **сетевого трафика** к **веб-серверу и от веб-сервера**.
FDP_IFC.2.2(1)	ФБО должны обеспечить **распространение фильтрации** на все операции перемещения **через МЭ** информации к **веб-серверу и от веб-сервера** распространялась **фильтрация**.
Зависимости:	FDP_IFF.1 Простые атрибуты безопасности.

FDP_IFC.2 (2)	**Полное управление информационными потоками**
FDP_IFC.2.1 (2)	ФБО должны осуществлять [фильтрацию] для [отправители информации, получатели информации, сетевой трафик] и всех операций перемещения **контролируемой МЭ** информации **сетевого трафика** к **веб-серверу и от веб-сервера, с учетом управляющих команд от взаимодействующих с МЭ средств защиты информации других видов**.

FDP_IFC.2.2 (2) ФБО должны обеспечить **распространение фильтрации** на все операции перемещения **через МЭ** информации к **веб-серверу и от веб-сервера** распространялась **фильтрация**.

Зависимости: FDP_IFF.1 Простые атрибуты безопасности.

FDP_IFF.1(1) Простые атрибуты безопасности

FDP_IFF.1.1 (1) ФБО должны осуществлять [фильтрацию], основанную на следующих типах атрибутов безопасности: [назначение: *список субъектов и типов информации, находящихся под управлением указанной политики, и для каждого из них – атрибуты безопасности*].

FDP_IFF.1.2 (1) ФБО должны разрешать информационный поток между управляемым субъектом и управляемой информацией посредством управляемой операции, если выполняются следующие правила: [нет].

FDP_IFF.1.3 (1) ФБО должны осуществлять:
[проверку наличия фрагментов мобильного кода в запросах пользователей к сайту и (или) иному веб-приложению на ввод данных путем поиска в таких запросах определенных фрагментов регулярных выражений (тегов, команд в формате языков мобильного кода), используемых при инициализации мобильного кода или выполнения нежелательных действий;
[назначение: *дополнительные правила политики управления информационными потоками*]].

FDP_IFF.1.4 (1) ФБО должны явно разрешать информационный поток, основываясь на следующих правилах:
[устанавливаемый администратором МЭ набор правил фильтрации, основанный на атрибутах, идентифицированных в FDP_IFF.1.1;
на основе результатов проверок в соответствии с FDP_IFF.1.3].

FDP_IFF.1.5 (1) ФБО должны явно запрещать информационный поток, основываясь на следующих правилах:
[устанавливаемый администратором МЭ набор правил фильтрации, основанный на атрибутах, идентифицированных в FDP_IFF.1.1;
обнаружение запроса пользователя к сайту и (или) иному веб-приложению на ввод данных, содержащий мобильный код, выявленный на основе результатов проверок в соответствии с FDP_IFF.1.3].

Зависимости: FDP_IFC.1 Ограниченное управление информационными потоками;
FMT_MSA.3 Инициализация статических атрибутов.

Замечание по применению: помимо указанных в элементе FDP_IFF.1.1(1) типов атрибутов безопасности информации дополнительно могут быть указаны иные типы информации и их атрибутов, например, разрешенные/запрещенные вложения электронных сообщений.

FDP_IFF.1(2) Простые атрибуты безопасности

FDP_IFF.1.1 (2) ФБО должны осуществлять [фильтрацию пакетов с учетом управляющих команд от средств защиты информации], основанную на следующих типах атрибутов безопасности субъекта и информации: [атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика].

FDP_IFF.1.2 (2) ФБО должны разрешать информационный поток между управляемым субъектом и управляемой информацией посредством управляемой операции, если выполняются следующие правила: [значения атрибутов индикации наличия признаков нарушения безопасности в информации сетевого трафика указывают на отсутствие нарушений].

FDP_IFF.1.3 (2) ФБО должны осуществлять [назначение: *дополнительные правила политики управления информационными потоками*].

FDP_IFF.1.4 (2) ФБО должны явно разрешать информационный поток, основываясь на следующих правилах: [назначение: *основанные на атрибутах безопасности правила, которые явно разрешают информационные потоки*].

FDP_IFF.1.5 (2) ФБО должны явно запрещать информационный поток, основываясь на следующих правилах: [значения атрибутов индикации наличия признаков нарушения безопасности в информации сетевого трафика указывают на наличие нарушений].

Зависимости: FDP_IFC.1 Ограниченное управление информационными потоками;
FMT_MSA.3 Инициализация статических атрибутов.

Замечание по применению: значения атрибутов, указывающих на наличие или отсутствие признаков нарушения безопасности в информации сетевого трафика, устанавливаются в соответствии с результатами работы соответствующих взаимодействующих средств защиты информации.

FDP_IFF.1(3) Простые атрибуты безопасности

FDP_IFF.1.1 (3) ФБО должны осуществлять [блокирование всех информационных потоков, проходящих через МЭ**], основанное** на следующих типах атрибутов безопасности **субъектов:** [атрибутах, указывающих на нарушение функционирования МЭ].

FDP_IFF.1.2 (3) ФБО должны разрешать информационный поток между управляемым субъектом и управляемой информацией посредством управляемой операции, если выполняются следующие правила: [нет].

FDP_IFF.1.3 (3) ФБО должны осуществлять [нет].

FDP_IFF.1.4 (3) ФБО должны явно разрешать информационный поток, основываясь на следующих правилах: [нет].

FDP_IFF.1.5 (3) ФБО должны явно запрещать информационный поток, основываясь на следующих правилах: [нарушение функционирования МЭ].

Зависимости: FDP_IFC.1 Ограниченное управление информационными потоками;
FMT_MSA.3 Инициализация статических атрибутов.

Замечание по применению: Нарушением функционирования МЭ должно считаться как некорректное функционирование, так и отсутствие признаков функционирования МЭ.

FDP_IFF_EXT.7 Базовая поддержка атрибутов протокола передачи гипертекста

FDP_IFF_EXT.7.1 ФБО должны поддерживать контроль и анализ запросов и ответов по протоколу передачи гипертекста следующих версий [назначение: *поддерживаемые версии протокола передачи гипертекста*].

FDP_IFF_EXT.7.2 ФБО должны поддерживать контроль и анализ сообщений, отправляемых веб-браузером веб-серверу и содержащих текстовый контент [назначение: *кодировки*] и нетекстовый контент [выбор: *изображения, аудиоинформацию, видеоинформацию, программы,* [назначение: *иные типы нетекстового контента*]].

FDP_IFF_EXT.7.3 ФБО должны поддерживать контроль и анализ куки [выбор: *временные куки, постоянные куки, сторонние куки,* [назначение: *иные типы куки*]], отправляемых веб-сервером веб-браузеру и возвращаемых веб-браузером веб-серверу, содержащих персонифицированную информацию сеанса взаимодействия пользователя с веб-сервером, основываясь на [выбор: *типах куки, сроке действия куки, версии куки, доменном имени веб-сервера, пути к запрашиваемому ресурсу*, [назначение: *иных атрибутах куки*]].

Зависимости: отсутствуют.

7.1.4. Управление безопасностью (FMT)

FMT_SMF.1 Спецификация функций управления

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

Зависимости: отсутствуют.

FMT_MTD.1 (1) Управление данными ФБО

FMT_MTD.1.1 (1) ФБО должны предоставлять возможность [выбор: *изменение значений по умолчанию, запрос, модификация, удаление, очистка,* [назначение: *другие операции*]] следующих данных [назначение: *список данных ФБО*] только [администраторам МЭ]].

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

FMT_MTD.1 (2) Управление данными ФБО

FMT_MTD.1.1 (2) ФБО должны предоставлять возможность [определения виртуализированных сетевых портов приложений], [сопоставления виртуализированных сетевых портов приложений с реальными сетевыми портами приложений] только [администраторам МЭ]].

Зависимости: FMT_SMR.1 Роли безопасности.

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 [администраторам МЭ]].

Зависимости: FMT_SMR.1 Роли безопасности.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:
[а) администратор МЭ;
б) [назначение: *другие роли*]].

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

Зависимости: FIA_UID.1 Выбор момента идентификации.

FMT_MSA.1 (1) Управление атрибутами безопасности

FMT_MSA.1.1 (1) ФБО должны **для осуществления** [фильтрации] **предоставлять** возможность *[назначать], модифицировать, удалять* [разрешительные и (или) запретительные] атрибуты безопасности [назначение: *список атрибутов безопасности*] только [администраторам МЭ].

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

FMT_MSA.1 (2) Управление атрибутами безопасности

FMT_MSA.1.1 (2) ФБО должны **для осуществления** [фильтрации] **предоставлять** возможность *[назначать], модифицировать, удалять* [разрешительные и (или) запретительные] атрибуты безопасности **для информации по протоколу передачи гипертекста** [администраторам МЭ].

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

7.1.5. Защита ФБО (FPT)

FPT_RCV.1 Ручное восстановление

FPT_RCV.1.1 После [назначение: *список сбоев/ прерываний обслуживания*] ФБО должны перейти в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

Зависимости: AGD_OPE.1 Руководство пользователя по эксплуатации.

FPT_TST.1 Тестирование ФБО

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

FPT_TST.1.2 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность [выбор: [назначение: *данных частей ФБО*], *данных ФБО*].

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

Зависимости: отсутствуют.

7.1.6. Специальные функции МЭ (FFW)

FFW_ARP_EXT.2 Блокирование передачи гипертекста

FFW_ARP_EXT.2.1 ФБО должны блокировать неразрешенный информационный поток по протоколу передачи гипертекста, путем
[выбор:
а) блокирования запроса по протоколу передачи гипертекста;
б) разрыва сетевого соединения;
в) перезапуска сетевого соединения;
г) блокирования взаимодействия с конкретным сетевым адресом;
д) блокирование сессии на уровне конкретного приложения;
е) блокирование взаимодействия на уровне конкретного пользователя приложения;
ж) отправка управляющего сигнала на иной МЭ для блокирования неразрешенного информационного потока;
з) [назначение: *другой способ*]].

FFW_ARP_EXT.2.2 ФБО должны уведомлять (оповещать) о выполненной блокировке *администратора МЭ*, [назначение: *иные уполномоченные роли*].

FFW_ARP_EXT.2.3 ФБО должны обеспечивать возможность отключения примененной блокировки информационных потоков
[выбор:
а) по запросу [назначение: *уполномоченные роли*];
б) [назначение: *иные условия отключения блокировки*]]
путем
[выбор:
а) полной отмены блокировки;
б) частичной отмены блокировки [выбор: *для отдельных типов запросов,* [назначение: *иные основания частичной отмены блокировки*]]].

Зависимости: отсутствуют.

FFW_EVP_EXT.1 Виртуализация внешнего представления приложений веб-сервера

FFW_EVP_EXT.1.1 ФБО должны поддерживать виртуализацию внешнего представления приложений веб-сервера на уровне: *трансляции сетевых портов;* [назначение: *другие способы виртуализации*].

Зависимости: отсутствуют.

Замечание по применению: Виртуализация внешнего представления приложений веб-сервера применяется с целью сокрытия реальных идентификационных признаков веб-сервера.

7.2. Требования доверия к безопасности объекта оценки

Требования доверия к безопасности ОО взяты из национального стандарта Российской Федерации 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» и образуют ОУД2, усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана» (см. таблицу 7.2.).

Таблица 7.2 – Требования доверия к безопасности ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Разработка	ADV_ARC.1	Описание архитектуры безопасности
	ADV_FSP.2	Детализация вопросов безопасности в функциональной спецификации
	ADV_IMP.2*	Полное отображение представления реализации ФБО
	ADV_IMP_EXT.3*	Реализация ОО
	ADV_TDS.3	Базовый модульный проект
Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_PRE.1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC.2	Использование системы УК
	ALC_CMS.2	Охват УК частей ОО

Продолжение таблицы 7.2

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
	ALC_DEL.1	Процедуры поставки
	ALC_FLR.1	Базовое устранение недостатков
	ALC_TAT_EXT.0	Определение инструментальных средств 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.1	Свидетельство покрытия
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2**	Выборочное независимое тестирование
Оценка уязвимостей	AVA_VAN.4	Методический анализ уязвимостей
Процедуры обновления программного обеспечения межсетевого экрана	ALC_FPU_EXT.1	Процедуры обновления программного обеспечения межсетевого экрана
Анализ влияния на безопасность	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность межсетевого экрана

* – 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).

** – В элементе ATE_IND.2.3E операция «уточнение» выполняется следующим образом:

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

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 (разработчика, производителя)

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

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

ADV_ARC.1.3D Заявитель (разработчик, производитель) должен предоставить «Описание архитектуры безопасности» ФБО.

Элементы содержания и представления документированных материалов

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, **поддерживаемых** ФБО **в соответствии** с ФТБ.

ADV_ARC.1.3C «Описание архитектуры безопасности» должно предоставлять информацию о том, **каким образом защищен** процесс инициализации ФБО.

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_ARC.1.1C – ADV_ARC.1.5C.

Замечания по применению: архитектура безопасности должна обеспечивать, чтобы МЭ не имел каналов связи, обеспечивающих доступ

(в том числе внеполосный) в обход заданных правил управления доступом к МЭ (его программному обеспечению и настройкам), а также правил контроля и фильтрации информационных потоков.

Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 10.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации

Зависимости: ADV_TDS.1 Базовый проект.

Элементы действий заявителя (разработчика, производителя)

ADV_FSP.2.1D Заявитель (разработчик, производитель) должен представить функциональную спецификацию.

ADV_FSP.2.2D Заявитель (разработчик, производитель) должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления документированных материалов

ADV_FSP.2.1C В функциональной спецификации должны быть полностью представлены ФБО.

ADV_FSP.2.2C В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV_FSP.2.3C В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV_FSP.2.4C Для каждого ИФБО, осуществляющего выполнение ФТБ, функциональная спецификация должна содержать описание связанных с данным ИФБО действий, осуществляющих выполнение ФТБ.

ADV_FSP.2.5C Для ИФБО, осуществляющих выполнение ФТБ, функциональная спецификация должна содержать описание сообщений о непосредственных ошибках, возникающих в результате функционирования, связанного с действиями, осуществляющими выполнение ФТБ.

ADV_FSP.2.6C В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий испытательной лаборатории

ADV_FSP.2.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_FSP.2.1C – ADV_FSP.2.6C.

ADV_FSP.2.2E Испытательная лаборатория должна сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 10.4.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

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 (разработчика, производителя)

ADV_IMP.2.1D Заявитель (разработчик, производитель) должен обеспечить доступ к представлению реализации для всех ФБО **на уровне исходных текстов всего программного обеспечения, входящего в состав ОО (с указанием в документации значений контрольных сумм файлов с исходными текстами ПО)**.

ADV_IMP.2.2D Заявитель (разработчик, производитель) должен обеспечить прослеживание всего представления реализации к описанию проекта ОО.

Элементы содержания и представления документированных материалов

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 всем представлением реализации и описанием проекта ОО **(для всех модулей, отнесенных к осуществляющим или поддерживающим выполнение ФТБ)** должно быть продемонстрировано их соответствие, а для **модулей изделия, определенных как «не влияющие на выполнение ФТБ», должно быть предоставлено соответствующее обоснование**.

Элементы действий испытательной лаборатории

ADV_IMP.2.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_IMP.2.1C – ADV_IMP.2.3C, **в том числе на основе результатов:**

а) контроля исходного состояния ПО;

б) контроля полноты и отсутствия избыточности исходных текстов на уровне файлов.

Замечания по применению:

1. В ADV_IMP.2.1E контроль исходного состояния ПО предусматривает фиксацию состава ПО и документации на него и сравнение с описанием, представленным в документации. При фиксации также должен быть выполнен 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 предусматривает анализ документированной информации, предоставленной заявителем (разработчиком, производителем) 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.

Испытательная лаборатория при контроле полноты исходных текстов должна исследовать (основываясь на структурном анализе и декомпозиции) модули, входящие в представление реализации, с тем, чтобы сделать заключение о соответствии их назначения описанию назначения (описанию выполняемых модулем функции), представленному в проекте ОО, и о достаточности представления реализации для выполнения ФТБ.

Испытательная лаборатория при контроле отсутствия избыточности исходных текстов должна:

в части модулей, осуществляющих и поддерживающих выполнение ФТБ – исследовать (основываясь на структурном анализе и декомпозиции) эти модули, чтобы сделать заключение об отсутствии в исходных текстах

функциональных возможностей безопасности, не предусмотренных проектом и ФТБ;

в части модулей, заявленных как «не влияющие на выполнение ФТБ» – проанализировать эти модули с глубиной, достаточной для подтверждения их невлияния на выполнение ФТБ.

ADV_IMP_EXT.3 Реализация ОО

Зависимости: ADV_IMP.2 Полное отображение представления реализации ФБО.

Элементы действий заявителя (разработчика, производителя)

ADV_IMP_EXT.3.1D Заявитель (разработчик, производитель) должен предоставить реализацию ОО.

ADV_IMP_EXT.3.2D Заявитель (разработчик, производитель) должен обеспечить прослеживание реализации ОО к представлению реализации ФБО.

Элементы содержания и представления документированных материалов

ADV_IMP_EXT.3.1C В документации должны быть указаны значения контрольных сумм элементов реализации ПО [выбор: *загрузочные модули ПО*, [назначение: *иные типы элементов реализации ПО*]].

ADV_IMP_EXT.3.2C В прослеживании между реализацией ОО и представлением реализации должно быть продемонстрировано [выбор:

а) для аппаратной платформы – соответствие между реализацией аппаратной платформы и ее представлением реализации [выбор: *схемы аппаратных средств, представления (кода) на языке описания аппаратных средств* [назначение: *иные формы представления реализации*]];

б) для ПО – соответствие между реализацией ПО [выбор: *загрузочные модули ПО*, [назначение: *иные типы элементов реализации ПО*]] и их представлением реализации [выбор: *исходные тексты ПО,* [назначение: *иные формы представления реализации*]]].

Элементы действий испытательной лаборатории

ADV_IMP_EXT.3.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_IMP_EXT.3.1C и ADV_IMP_EXT.3.2C.

ADV_TDS.3 Базовый модульный проект

Зависимости: ADV_FSP.4 Полная полуформальная функциональная спецификация.

Элементы действий заявителя (разработчика, производителя)

ADV_TDS.3.1D Заявитель (разработчик, производитель) должен представить проект ОО.

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

Элементы содержания и представления документированных материалов

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_TDS.3.1C – ADV_TDS.3.10C.

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

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 10.8.3 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.2. Руководства (AGD)

AGD_OPE.1 Руководство пользователя по эксплуатации

Зависимости: ADV_FSP.1 Базовая функциональная спецификация.

Элементы действий заявителя (разработчика, производителя)

AGD_OPE.1.1D Заявитель (разработчик, производитель) должен представить руководство пользователя по эксплуатации.

Элементы содержания и представления документированных материалов

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 **необходимых** 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, **в частности** 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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AGD_OPE.1.1C – AGD_OPE.1.7C.

Замечания по применению: материал, соответствующий пользовательским ролям по администрированию МЭ, включается в «Руководство администратора». Материал, соответствующий иным пользовательским ролям, включается в «Руководство пользователя».

Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 11.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

AGD_PRE.1 Подготовительные процедуры

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

AGD_PRE.1.1D Заявитель (разработчик, производитель) должен предоставить ОО вместе с подготовительными процедурами.

Элементы содержания и представления документированных материалов

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

AGD_PRE1.2C В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки **и настройки** 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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AGD_PRE1.1C и AGD_PRE1.2C.

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

Замечания по применению: материал подготовительных процедур включается в «Руководство администратора», детализация подготовительных процедур в части безопасной настройки МЭ – в «Правила по безопасной настройке».

Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 11.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.3. Поддержка жизненного цикла (ALC)

ALC_CMC.2 Использование системы УК

Зависимости: ALC_CMS.1 Охват УК ОО

Элементы действий заявителя (разработчика, производителя)

ALC_CMC.2.1D Заявитель (разработчик, производитель) должен предоставить ОО и маркировку для ОО.

ALC_CMC.2.2D Заявитель (разработчик, производитель) должен предоставить документацию УК.

ALC_CMC.2.3D Заявитель (разработчик, производитель) должен использовать систему УК.

Элементы содержания и представления документированных материалов

ALC_CMC.2.1C ОО должен быть помечен уникальной маркировкой.

ALC_CMC.2.2C В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.

ALC_CMC.2.3C В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.

Элементы действий испытательной лаборатории

ALC_CMC.2.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_CMC.2.1C – ALC_CMC.2.3C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 12.2.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_CMS.2 Охват УК частей ОО

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_CMS.2.1D Заявитель (разработчик, производитель) должен представить список элементов конфигурации для ОО.

Элементы содержания и представления документированных материалов

ALC_CMS.2.1C Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по требованиям доверия к безопасности, а также части, которые входят в состав ОО.

ALC_CMS.2.2C Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC_CMS.2.3C Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

Элементы действий испытательной лаборатории

ALC_CMS.2.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_CMS.2.1C – ALC_CMS.2.3C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 12.3.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения

безопасности. Методология оценки безопасности информационных технологий».

ALC_DEL.1 Процедуры поставки

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_DEL.1.1D Заявитель (разработчик, производитель) должен задокументировать процедуры поставки ОО или его частей потребителю.

ALC_DEL.1.2D Заявитель (разработчик, производитель) должен использовать процедуры поставки.

Элементы содержания и представления документированных материалов

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DEL.1.1C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 12.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_FLR.1 Базовое устранение недостатков

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_FLR.1.1D Заявитель (разработчик, производитель) должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

Элементы содержания и представления документированных материалов

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_FLR.1.1C – ALC_FLR.1.4C.

Замечания по применению: для выполнения данных требований заявитель (разработчик, производитель) должен осуществлять постоянный поиск и устранение уязвимостей и других недостатков в МЭ и выпуск соответствующих обновлений программной части МЭ.

Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 12.6.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.4. Оценка задания по безопасности (ASE)

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 (разработчика, производителя)

ASE_CCL.1.1D Заявитель (разработчик, производитель) должен представить **в ЗБ** «Утверждения о соответствии».

ASE_CCL.1.2D Заявитель (разработчик, производитель) должен представить **в ЗБ** «Обоснование утверждений о соответствии».

Элементы содержания и представления документированной информации

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

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

ASE_CCL.1.3C В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ПЗ ГОСТ Р ИСО/МЭК 15408-3; ЗБ либо описывается как соответствующее требованиям ГОСТ Р ИСО/МЭК 15408-3, либо как содержащее расширенные по отношению к ГОСТ Р ИСО/МЭК 15408-3 требования **(специальные 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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_CCL.1.1C – ASE_CCL.1.10C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_ECD.1 Определение расширенных компонентов

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ASE_ECD.1.1D Заявитель (разработчик, производитель) должен представить **в ЗБ** изложение «Требований безопасности».

ASE_ECD.1.2D Заявитель (разработчик, производитель) должен представить **в ЗБ** «Определение расширенных компонентов».

Элементы содержания и представления документированных материалов

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

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

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

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

ASE_ECD.1.5C Расширенные **(специальные)** компоненты должны состоять из измеримых объективных элементов, **обеспечивающих** возможность **демонстрации соответствия** или **несоответствия** этим элементам.

Элементы действий испытательной лаборатории

ASE_ECD.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_ECD.1.1C – ASE_ECD.1.5C.

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

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.7.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_INT.1 Введение Задания по безопасности

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ASE_INT.1.1D Заявитель (разработчик, производитель) ЗБ должен представить **в ЗБ** «Введение ЗБ».

Элементы содержания и представления документированных материалов

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_INT.1.1C – ASE_INT.1.8C.

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

Замечания по применению: Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_OBJ.2 Цели безопасности

Зависимости: ASE_SPD.1 Определение проблемы безопасности.

Элементы действий заявителя (разработчика, производителя)

ASE_OBJ.2.1D Заявитель (разработчик, производитель) должен предоставить **в ЗБ** «Определение целей безопасности».

ASE_OBJ.2.2D Заявитель (разработчик, производитель) должен предоставить **в ЗБ** «Обоснование целей безопасности».

Элементы содержания и представления документированных материалов

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 политикам безопасности, 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 политикам безопасности, 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 политик безопасности.

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_OBJ.2.1C – ASE_OBJ.2.6C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.6.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_REQ.2 Производные требования безопасности

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

Элементы действий заявителя (разработчика, производителя)

ASE_REQ.2.1D Заявитель (разработчик, производитель) должен представить **в ЗБ изложение** «Требований безопасности».

ASE_REQ.2.2D Заявитель (разработчик, производитель) должен представить **в ЗБ** «Обоснование требований безопасности».

Элементы содержания и представления документированных материалов

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 **быть выполнены** 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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_REQ.2.1C – ASE_REQ.2.9C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.8.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_SPD.1 Определение проблемы безопасности

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ASE_SPD.1.1D Заявитель (разработчик, производитель) должен представить **в ЗБ** «Определение проблемы безопасности».

Элементы содержания и представления документированных материалов

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 политики безопасности.

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_SPD.1.1C – ASE_SPD.1.4C.

Замечания по применению: Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.5.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

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 (разработчика, производителя)

ASE_TSS.1.1D Заявитель (разработчик, производитель) должен представить **в ЗБ** «Краткую спецификацию ОО».

Элементы содержания и представления документированных материалов

ASE_TSS.1.1C «Краткая спецификация ОО» должна описывать, каким образом ОО выполняет каждое ФТБ, **а также описывать меры доверия, направленные на реализацию ТДБ**.

Элементы действий испытательной лаборатории

ASE_TSS.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_TSS.1.1C.

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

Замечания по применению: Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.9.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий». Дополнительно должно быть проанализировано покрытие ТДБ мерами доверия.

7.2.5 Тестирование (ATE)

ATE_COV.1 Свидетельство покрытия

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

Элементы действий заявителя (разработчика, производителя)

ATE_COV.1.1D Заявитель (разработчик, производитель) должен представить свидетельство покрытия тестами.

Элементы содержания и представления документированных материалов

ATE_COV.1.1C Свидетельство покрытия тестами должно демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.

Элементы действий испытательной лаборатории

ATE_COV.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ATE_COV.1.1C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 13.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ATE_FUN.1 Функциональное тестирование

Зависимости: ATE_COV.1 Свидетельство покрытия.

Элементы действий заявителя (разработчика, производителя)

ATE_FUN.1.1D Заявитель (разработчик, производитель) должен протестировать ФБО и задокументировать результаты.

ATE_FUN.1.2D Заявитель (разработчик, производитель) должен представить тестовую документацию.

Элементы содержания и представления документированных материалов

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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ATE_FUN.1.1C – ATE_FUN.1.4C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 13.5.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

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 (разработчика, производителя)

ATE_IND.2.1D Заявитель (разработчик, производитель) должен представить ОО для тестирования.

Элементы содержания и представления документированных материалов

ATE_IND.2.1C ОО должен быть пригоден для тестирования.

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

Элементы действий испытательной лаборатории

ATE_IND.2.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ATE_IND.2.1C и ATE_IND.2.2C.

ATE_IND.2.2E Испытательная лаборатория должна выполнить выборку тестов из тестовой документации в целях верификации результатов тестирования, полученных разработчиком.

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

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 13.6.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.6. Оценка уязвимостей (AVA)

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 (разработчика, производителя)

AVA_VAN.4.1D Заявитель (разработчик, производитель) должен **выполнить анализ уязвимостей**.

Элементы содержания и представления документированных материалов

AVA_VAN.4.1C **Документация анализа уязвимостей должна:**
а) содержать результаты анализа, выполненного для поиска способов, которыми потенциально может быть нарушена реализация ФТБ;
б) идентифицировать проанализированные предполагаемые уязвимости;
в) 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 информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AVA_VAN.4.1C.

AVA_VAN.4.2E Испытательная лаборатория должна выполнить поиск информации в общедоступных источниках **в целях идентификации потенциальных уязвимостей** 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, **в целях оформления заключения о стойкости** ОО к нападениям, выполняемым нарушителем, обладающим **Умеренным** потенциалом нападения.

Замечания по применению:

1. Испытательная лаборатория должна исследовать базы данных об уязвимостях в сети Интернет, национальную базу данных (если применимо), информацию, полученную от органа по сертификации (если применимо). Для выявления уязвимостей также необходимо использовать национальные стандарты по классификации уязвимостей и порядку выполнения работ по выявлению и оценке уязвимостей.

2. Наиболее тщательно должны быть подготовлены и проведены тесты проникновения, связанные с тестированием уязвимостей, которые потенциально могут быть использованы нарушителем для обхода, отключения или преодоления функций безопасности СЗИ, реализующих основные функциональные возможности СЗИ, определяемые видом и типом СЗИ.

3. Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 14.2.4 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.7. Требования к объекту оценки, сформулированные в явном виде

ALC_TAT_EXT.0 Определение инструментальных средств разработки

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_TAT_EXT.0.1D Заявитель (разработчик, производитель) должен идентифицировать инструментальные средства, использованные при разработке **(производства)** МЭ.

ALC_TAT_EXT.0.2D Заявитель (разработчик, производитель) должен задокументировать опции инструментальных средств разработки **(производства)**, использованные при разработке МЭ.

Элементы содержания и представления документированных материалов

ALC_TAT_EXT.0.1C В документированных материалах должны быть идентифицированы инструментальные средства, использовавшиеся при разработке МЭ.

ALC_TAT_EXT.0.2C В документированных материалах должны быть отражены опции инструментальных средств разработки **(производства)**, использованные при разработке МЭ.

Элементы действий испытательной лаборатории

ALC_TAT_EXT.0.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ALC_TAT_EXT.0.1C, ALC_TAT_EXT.0.2C.

Замечания по применению: иерархическим для ALC_TAT_EXT.0 является ALC_TAT.1 «Полностью определенные инструментальные средства разработки»

ALC_FPU_EXT.1 Процедуры обновления программного обеспечения межсетевого экрана

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_FPU_EXT.1.1D Заявитель (разработчик, производитель) должен разработать и реализовать технологию обновления МЭ для [назначение: *типы обновлений*].

ALC_FPU_EXT.1.2D Заявитель (разработчик, производитель) должен разработать и поддерживать регламент обновления программного обеспечения МЭ.

ALC_FPU_EXT.1.3D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру уведомления потребителей о выпуске обновлений МЭ, основанную на [назначение: *способы уведомления*].

ALC_FPU_EXT.1.4D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру предоставления обновлений потребителям МЭ, основанную на [назначение: *способы предоставления обновлений*].

ALC_FPU_EXT.1.5D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру представления обновлений в испытательную лабораторию для проведения внешнего контроля, основанную на [назначение: *способы предоставления обновлений для контроля*].

Элементы содержания и представления документированных материалов

ALC_FPU_EXT.1.1C Документация МЭ должна содержать описание технологии выпуска обновлений МЭ.

ALC_FPU_EXT.1.2C Документация МЭ должна содержать регламент обновления МЭ, включающий:

а) идентификацию типов выпускаемых обновлений;

б) описание процедуры уведомления потребителей о выпуске обновлений;

в) описание процедуры предоставления обновлений потребителям;

г) описание содержания эксплуатационной документации на выпускаемые обновления;

д) [назначение: *иная информация*].

ALC_FPU_EXT.1.3C Регламент обновления МЭ должен предусматривать включение в эксплуатационную документацию на выпускаемые обновление описания следующих процедур:

а) процедуры получения обновления;

б) процедуры контроля целостности обновления;

в) типовой процедуры тестирования обновления;
г) процедуры установки и применения обновления;
д) процедуры контроля установки обновления;
е) процедуры верификации (проверки) применения обновления.

ALC_FPU_EXT.1.4C Документация процедуры представления обновлений для проведения внешнего контроля должна содержать:
а) описание процедуры предоставления обновлений для внешнего контроля;
б) требования к предоставлению и содержанию методики тестирования обновления заявителем;
в) требования к оформлению и предоставлению результатов тестирования обновления заявителем;
г) [назначение: *иная информация*].

Элементы действий испытательной лаборатории

ALC_FPU_EXT.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ALC_FPU_EXT.1.1C - ALC_FPU_EXT.1.4C.

ALC_FPU_EXT.1.2E Испытательная лаборатория должна проверить, что процедура представления обновлений для проведения внешнего контроля позволяет организовать и проводить их внешний контроль.

Замечания по применению: в качестве типов обновлений рассматриваются: обновления, направленные на устранение уязвимостей ОО; иные обновления, оказывающие влияние на безопасность ОО; обновления, не оказывающие влияния на безопасность ОО.

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность межсетевого экрана

Зависимости: ALC_FPU_EXT.1 Процедуры обновления программного обеспечения межсетевого экрана.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность МЭ должны содержать краткое описание влияния обновлений на задание по безопасности, **реализацию МЭ функциональных возможностей** или логическое обоснование отсутствия такого влияния, **подтверждение устранения уязвимости (уязвимостей), на устранение которой (которых) направлен выпуск данных обновлений и невнесения иных уязвимостей в МЭ**.

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

Элементы действий испытательной лаборатории

AMA_SIA_EXT.3.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в AMA_SIA_EXT.3.1C, AMA_SIA_EXT.3.2C.

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

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**	**Цель безопасности-7**	**Цель безопасности-8**	**Цель безопасности-9**	**Цель безопасности-10**
FAU_ARP.1								**X**		
FAU_GEN.1						**X**				
FAU_SAR.1						**X**				
FAU_SEL.1						**X**				
FIA_UAU.2					**X**					
FIA_UID.2					**X**					
FDP_IFC.2	**X**	**X**								
FDP_IFF.1	**X**	**X**								
FDP_IFF_EXT.7	**X**									
FMT_MOF.1				**X**						
FMT_MTD.1				**X**						
FMT_SMF.1				**X**						
FMT_SMR.1			**X**							
FMT_MSA.1	**X**									
FPT_RCV.1							**X**			
FPT_TST.1							**X**			
FFW_ARP_EXT.2									**X**	
FFW_EVP_EXT.1										**X**

Включение указанных в таблице 7.3 функциональных требований безопасности ОО в ПЗ определяется Требованиями к межсетевым экранам, утвержденными приказом ФСТЭК России от 9 февраля 2016 г. № 9.

FAU_ARP.1 Сигналы нарушения безопасности

Выполнение требований данного компонента обеспечивает возможность выполнения действий по оповещению уполномоченных лиц, в том числе – сигнализировать о событиях безопасности, связанных с обнаружением неразрешенных информационных потоков по протоколу передачи гипертекста, при обнаружении критичных событий безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-8** 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 предоставления администратору всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, потенциально подвергаемых аудиту. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает аутентификацию пользователей до разрешения любых действий. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FIA_UID.2(1) Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает идентификацию пользователей до разрешения любых действий. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FIA_UID.2(2) Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает идентификацию субъектов межсетевого взаимодействия до разрешения передачи через МЭ информационного потока, ассоциированного с этим пользователем, к веб-серверу (от веб-сервера). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FDP_IFC.2(1) Полное управление информационными потоками

Выполнение требований данного компонента обеспечивает возможность осуществлять фильтрацию для отправителей информации, получателей информации, сетевого трафика и всех операций перемещения контролируемой МЭ информации сетевого трафика к веб-серверу и от веб-сервера, а также возможность обеспечения распространения фильтрации на все операции перемещения через МЭ информации к веб-серверу и от веб-сервера. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FDP_IFC.2(2) Полное управление информационными потоками

Выполнение требований данного компонента обеспечивает возможность фильтрации пакетов с учетом управляющих команд от взаимодействующих с МЭ средств защиты информации других видов. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FDP_IFF.1(1) Простые атрибуты безопасности

Выполнение требований данного компонента обеспечивает: возможность осуществлять фильтрацию, основанную на определенных типах атрибутов безопасности; осуществлять проверку наличия фрагментов мобильного кода в запросах пользователей к сайту и (или) иному веб-приложению на ввод данных путем поиска в таких запросах определенных фрагментов регулярных выражений (тегов, команд в формате языков мобильного кода), используемых при инициализации мобильного кода или выполнения нежелательных действий; возможность запрещать информационный поток, если в нем обнаружен запрос пользователя к сайту и (или) иному веб-приложению на ввод данных, содержащий выявленный мобильный код Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FDP_IFF.1(2) Простые атрибуты безопасности

Выполнение требований данного компонента обеспечивает возможность осуществлять фильтрацию пакетов с учетом управляющих команд от средств защиты информации, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FDP_IFF.1(3) Простые атрибуты безопасности

Выполнение требований данного компонента обеспечивает возможность блокирования всех информационных потоков, проходящих через нефункционирующий или функционирующий некорректно МЭ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FDP_IFF_EXT.7 Базовая поддержка атрибутов протокола передачи гипертекста

Выполнение требований данного компонента обеспечивает: возможность поддержки контроля и анализа запросов и ответов по протоколу передачи гипертекста определенных версий; возможность поддержки контроля и анализа сообщений, отправляемых веб-браузером веб-серверу и содержащих текстовый контент определенных кодировок и нетекстовый контент определенных типов (изображения, аудиоинформация, видеоинформация, программы); возможность поддержки контроля и анализа специальных маркеров взаимодействия (куки) определенных типов, отправляемых веб-сервером веб-браузеру и возвращаемых веб-браузером

веб-серверу, содержащих персонифицированную информацию сеанса взаимодействия пользователя с веб-сервером, основываясь на определенных атрибутах куки. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_MOF.1 Управление режимом выполнения функций безопасности

Выполнение требований данного компонента обеспечивает разрешение ФБО на модификацию режима выполнения функций МЭ администраторам и другим уполномоченным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FMT_MTD.1 Управление данными функций безопасности

Выполнение требований данного компонента предоставляет возможность со стороны администраторов управлять данными (данными МЭ), используемыми функциями безопасности МЭ, только администраторам МЭ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FMT_SMF.1 Спецификация функций управления

Выполнение требований данного компонента обеспечивает наличие у ОО, как минимум, функций управления режимом выполнения функций безопасности и функций управления данными ФБО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FMT_SMR.1 Роли безопасности

Выполнение требований данного компонента обеспечивает поддержание ролей безопасности и их ассоциации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FMT_MSA.1 (1) Управление атрибутами безопасности

Выполнение требований данного компонента предоставляет возможность администраторам МЭ назначать, модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для осуществления фильтрации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_MSA.1 (2) Управление атрибутами безопасности

Выполнение требований данного компонента предоставляет возможность администраторам МЭ назначать, модифицировать, удалять разрешительные и (или) запретительные атрибуты для информации по протоколу передачи гипертекста для осуществления фильтрации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FPT_RCV.1 Автоматическое восстановление без недопустимой потери

Выполнение требований данного компонента обеспечивает возможность перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FPT_TST.1 Тестирование функциональных возможностей безопасности

Выполнение требований данного компонента обеспечивает возможность тестирования (самотестирования) функций безопасности МЭ (контроль целостности исполняемого кода МЭ). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FFW_ARP_EXT.2 Блокирование передачи гипертекста

Выполнение требований данного компонента обеспечивает: возможность отправки управляющего сигнала на иной МЭ (тип «А») для блокирования неразрешенного информационного потока; возможность уведомления (оповещения) администратора МЭ о выполненной блокировке неразрешенного информационного потока по протоколу передачи гипертекста; возможность отключения примененной блокировки информационных потоков администратором МЭ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-9** и способствует ее достижению.

FFW_EVP_EXT.1 Виртуализация внешнего представления приложений

Выполнение требований данного компонента обеспечивает: возможность поддержки виртуализации внешнего представления приложений веб-сервера на уровне трансляции сетевых портов. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-10** 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 национальном стандарте 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» под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в национальном стандарте 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» под рубрикой «Зависимости».

Столбец 2 таблицы 7.4 является справочным и содержит компоненты, определенные в национальном стандарте 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» 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

Функциональные компоненты	**Зависимости в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 7.1 настоящего ПЗ**	**Удовлетворение зависимостей**
FAU_GEN.1	FPT_STM.1	Цель для среды функционирования ОО-8
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 FMT_MTD.1
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2 FMT_MSA.1
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_MTD.3	FMT_MTD.1	FMT_MTD.1
FMT_MSA.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RCV.1	AGD_OPE.1	AGD_OPE.1

Для компонента FAU_GEN.1 невключение по зависимости компонента FPT_STM.1 компенсировано включением в ПЗ Цели для среды функционирования ОО-8.

Компонент FDP_IFF.1 «Простые атрибуты безопасности» имеет зависимости от компонентов FMT_MSA.3 «Инициализация статических атрибутов» и FMT_MSA.1 «Управление атрибутами безопасности».

Компонент FMT_MSA.1 «Управление атрибутами безопасности» включен в настоящий ПЗ. Компонент FMT_MSA.3 «Инициализация статических атрибутов» не включен в настоящий ПЗ, чтобы не ограничивать реализацию присвоения ограничительных/разрешительных и других типов значений для атрибутов безопасности. При разработке ЗБ в зависимости от реализации ФБО должен использоваться компонент FMT_MSA.3 «Инициализация статических атрибутов» или иной компонент функциональных требований безопасности (допустимо использовать компонент, сформулированный в явном виде).

7.3.2. Обоснование требований доверия к безопасности объекта оценки

Требования доверия настоящего ПЗ соответствуют ОУД2, усиленному компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», и расширенному компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана».

Включение указанных требований доверия к безопасности ОО в ПЗ определяется Требованиями к межсетевым экранам, утвержденными приказом ФСТЭК России от 9 февраля 2016 г. № 9.

_____