ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утверждён ФСТЭК России
12 сентября 2016 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ МЕЖСЕТЕВЫХ ЭКРАНОВ ТИПА «Г» ШЕСТОГО КЛАССА ЗАЩИТЫ

ИТ.МЭ.Г6.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» шестого класса защиты.
Тип МЭ:	МЭ типа «Г».
Класс защиты:	Шестой.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.МЭ.Г6.ПЗ.
Идентификация ОО:	МЭ типа «Г» шестого класса защиты.
Уровень доверия:	Оценочный уровень доверия 1 (ОУД1), расширенный компонентами 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, ОУД1.

2.2. Аннотация профиля защиты

Настоящий ПЗ определяет требования безопасности для 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 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 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 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 обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования;

поддержка определенных ролей по управлению МЭ;

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

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

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 1 (ОУД1), расширенный компонентами 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 требований 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» (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»).

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 1 (ОУД1), расширенный компонентами 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. Цели безопасности

4.1. Цели безопасности для среды функционирования

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

Цель для среды функционирования ОО-1

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 объектом оценки в соответствии с эксплуатационной документацией.

Цель для среды функционирования ОО-7

Требования к персоналу

Персонал, ответственный за функционирование объекта оценки, должен обеспечивать надлежащее 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 надлежащего 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. Определение расширенных компонентов

В данном разделе ПЗ представлены расширенные компоненты для МЭ.

5.1. 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).

5.1.1. 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]*].

5.1.2. 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]]*]**.

5.2. Определение расширенных компонентов требований доверия к безопасности объекта оценки

Для МЭ типа «Г» определены следующие расширенные (специальные) компоненты требований доверия к безопасности: 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».

5.2.1. 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.

5.2.2. 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.

6. Требования безопасности

В данном разделе ПЗ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из ГОСТ Р ИСО/МЭК 15408-2-2013 «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 ОУД1, расширенного компонентами ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана». Требования безопасности 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»).

6.1. 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 6.1.

Таблица 6.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
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

6.1.1. Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на *минимальном* уровне аудита;

в) [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.

6.1.2. 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 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы **администратор МЭ** был успешно идентифицирован до разрешения **любого действия**, выполняемого при посредничестве ФБО от имени этого **администратора МЭ.**

Зависимости: отсутствуют.

6.1.3. 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 политика 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.

6.1.4. 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 Управление данными ФБО

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

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

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.

6.1.5. 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 МЭ к безопасному состоянию.

Зависимости: AGD_OPE.1 Руководство пользователя по эксплуатации.

6.1.6. 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.

6.2. Обоснование удовлетворения зависимостей функциональных требований безопасности

В таблице 6.2 представлены результаты удовлетворения зависимостей функциональных требований безопасности. Все зависимости компонентов требований удовлетворены в настоящем профиле защиты либо включением компонентов, определенных в 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 6.2 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 6.2, под рубрикой «Зависимости».

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

Таблица 6.2 - Зависимости функциональных требований безопасности

Функциональные компоненты	**Зависимости в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 6.1 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_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).

6.3. Требования доверия к безопасности

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 ОУД1, расширенный компонентами ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана» (см. таблицу 6.3.).

Таблица 6.3 – Требования доверия к безопасности ОО

Классы доверия	**Идентификаторы компонентов доверия**	**Названия компонентов доверия**
Разработка	ADV_FSP.1	Базовая функциональная спецификация
Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_PRE.1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC.1	Маркировка ОО
	ALC_CMS.1	Охват УК объекта оценки
Оценка задания по безопасности	ASE_CCL.1	Утверждения о соответствии
	ASE_ECD.1	Определение расширенных компонентов
	ASE_INT.1	Введение ЗБ
	ASE_OBJ.1	Цели безопасности для среды функционирования
	ASE_REQ.1	Установленные требования безопасности
	ASE_TSS.1	Краткая спецификация ОО
Тестирование	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_VAN.1	Обзор уязвимостей
Процедуры обновления программного обеспечения МЭ	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

6.3.1. Разработка (ADV)

ADV_FSP.1 Базовая функциональная спецификация

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ADV_FSP.1.1D Заявитель (разработчик, производитель) должен представить функциональную спецификацию.

ADV_FSP.1.2D Заявитель (разработчик, производитель) должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления документированных материалов

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

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

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

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

Элементы действий испытательной лаборатории

ADV_FSP.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_FSP.1.1C – ADV_FSP.1.4C.

ADV_FSP.1.2E 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 10.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

6.3.2. 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».

6.3.3 Поддержка жизненного цикла (ALC)

ALC_CMC.1 Маркировка ОО

Зависимости: ALC_CMS.1 Охват УК ОО.

Элементы действий заявителя (разработчика, производителя)

ALC_CMC.1.1D Заявитель (разработчик, производитель) должен предоставить ОО и маркировку для ОО.

Элементы содержания и представления документированных материалов

ALC_CMC.1.1C ОО должен быть помечен уникальной маркировкой.

Элементы действий испытательной лаборатории

ALC_CMC.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_CMC.1.1C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 12.2.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_CMS.1 Охват УК объекта оценки

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_CMS.1.1D Заявитель (разработчик, производитель) должен представить список элементов конфигурации для ОО.

Элементы содержания и представления документированных материалов

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

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

Элементы действий испытательной лаборатории

ALC_CMS.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_CMS.1.1C и ALC_CMS.1.2C.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 12.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

6.3.4. 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 документированных материалов

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.1 Цели безопасности для среды функционирования

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ASE_OBJ.1.1D Разработчик должен представить изложение **в ЗБ** «Целей безопасности».

Элементы содержания и представления документированных материалов

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

Элементы действий испытательной лаборатории

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

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 9.6.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_REQ.1 Установленные требования безопасности

Зависимости: ASE_ECD.1 Определение расширенных компонентов.

Элементы действий заявителя (разработчика, производителя)

ASE_REQ.1.1D Разработчик должен представить **в ЗБ изложение** «Требований безопасности».

ASE_REQ.1.2D Разработчик должен представить **в ЗБ** «Обоснование требований безопасности».

Элементы содержания и представления документированных материалов

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

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

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

ASE_REQ.1.4C Все операции должны выполняться **быть выполнены** правильно.

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

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

Элементы действий испытательной лаборатории

ASE_REQ.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_REQ.1.1C – ASE_REQ.1.6C.

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_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 краткую спецификацию ОО.

Элементы содержания и представления документированных материалов

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».

6.3.5. Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

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

Элементы действий заявителя (разработчика, производителя)

ATE_IND.1.1D Заявитель (разработчик, производитель) должен представить ОО для тестирования.

Элементы содержания и представления документированных материалов

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий испытательной лаборатории

ATE_IND.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_IND.1.1C.

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

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 13.6.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

6.3.6. Оценка уязвимостей (AVA)

AVA_VAN.1 Обзор уязвимостей

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

Элементы действий заявителя (разработчика, производителя)

AVA_VAN.1.1D Заявитель (разработчик, производитель) должен **выполнить анализ уязвимостей**.

Элементы содержания и представления документированных материалов

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

AVA_VAN.1.2E Испытательная лаборатория должна выполнить поиск информации в общедоступных источниках **в целях идентификации потенциальных уязвимостей** в ОО.

AVA_VAN.1.3E Испытательная лаборатория должна провести тестирование проникновения, основанное на идентифицированных уязвимостях, **в целях оформления заключения о стойкости** ОО к нападениям, выполняемым нарушителем, обладающим Базовым потенциалом нападения.

Замечания по применению: испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 14.2.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

6.3.7. Требования к объекту оценки, сформулированные в явном виде

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.
