ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утверждён ФСТЭК России
11 мая 2017 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ ТИПА «В» ШЕСТОГО КЛАССА ЗАЩИТЫ

ИТ.ОС.В6.ПЗ

2017

Содержание

Перечень сокращений

ЗБ – задание по безопасности
ИС – информационная система
ИТ – информационная технология
ИФБО – интерфейс функциональных возможностей безопасности ОО
ОО – объект оценки
ОС – операционная система
ОУД – оценочный уровень доверия
ПБО – политика безопасности организации
ПЗ – профиль защиты
ПО – программное обеспечение
ПФБ – политика функций безопасности
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 операционных систем на соответствие Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19 августа 2016 г. № 119.

Настоящий методический документ ФСТЭК России детализирует и определяет взаимосвязи требований и функций безопасности операционных систем (далее – ОС), установленных Требованиями безопасности информации к ОС, утвержденными приказом ФСТЭК России от 19 августа 2016 г. № 119.

Профиль защиты учитывает положения 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 сведения о профиле защиты (далее – ПЗ), которые предоставляют маркировку и описательную информацию, необходимую для контроля и идентификации ПЗ и объекта оценки (далее – 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 операционных систем типа «В» шестого класса защиты.
Тип ОС:	ОС типа «В».
Класс защиты:	Шестой.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.ОС.В6.ПЗ.
Идентификация ОО:	ОС типа «В» шестого класса защиты.
Уровень доверия:	Оценочный уровень доверия 1 (ОУД1), усиленный компонентами ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS.1 «Базовый проект» и расширенный компонентами ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы» и AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы».
Идентификация:	Требования безопасности информации к операционным системам, утвержденные приказом ФСТЭК России от 19 августа 2016 г. № 119. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
Ключевые слова:	Операционные системы, ОС реального времени.

2.2. Аннотация профиля защиты

Настоящий ПЗ определяет требования безопасности к операционным системам реального времени (тип «В») шестого класса защиты.

2.2.1. Ключевые термины, используемые в профиле защиты

Ниже приведены ключевые термины, используемые в профиле защиты при задании требований безопасности ОС и относящиеся к различным категориям пользователей ОС и субъектов доступа, и их определения.

Администратор: пользователь ОС, уполномоченный выполнять некоторые действия по администрированию ОС (имеющий административные полномочия) в соответствии с установленной ролью и требуемыми привилегиями в ОС на выполнение этих действий.

Непривилегированный субъект доступа: процесс, порождаемый пользователем.

Неуполномоченный субъект доступа: процесс, порождаемый лицами, не являющимися пользователями ОС, при попытке несанкционированного доступа.

Объект доступа: единица информационного ресурса (файл, каталог, том, устройство и (или) иные), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Пользователь: пользователь ОС, не имеющий административных полномочий.

Пользователь ОС: лицо (администратор, пользователь), которому разрешено выполнять некоторые действия (операции) по администрированию ОС или обработке информации в ОС.

Привилегированный субъект доступа: процесс, порождаемый администратором или от имени служебной учетной записи ОС.

Роль: предопределенная совокупность правил, устанавливающих допустимое взаимодействие с ОС.

Субъект доступа: процесс, порождаемый пользователем ОС (пользователем или администратором).

Уполномоченный непривилегированный субъект доступа: процесс, порождаемый пользователем в соответствии с правами доступа к объекту доступа.

Уполномоченный привилегированный субъект доступа: процесс, порождаемый администратором или от имени служебной учетной записи в соответствии с ролью.

Соотношение терминов, применяемых в настоящем профиле защиты для обозначения пользователей ОС и субъектов доступа различных категорий представлено на рисунке 2.1.

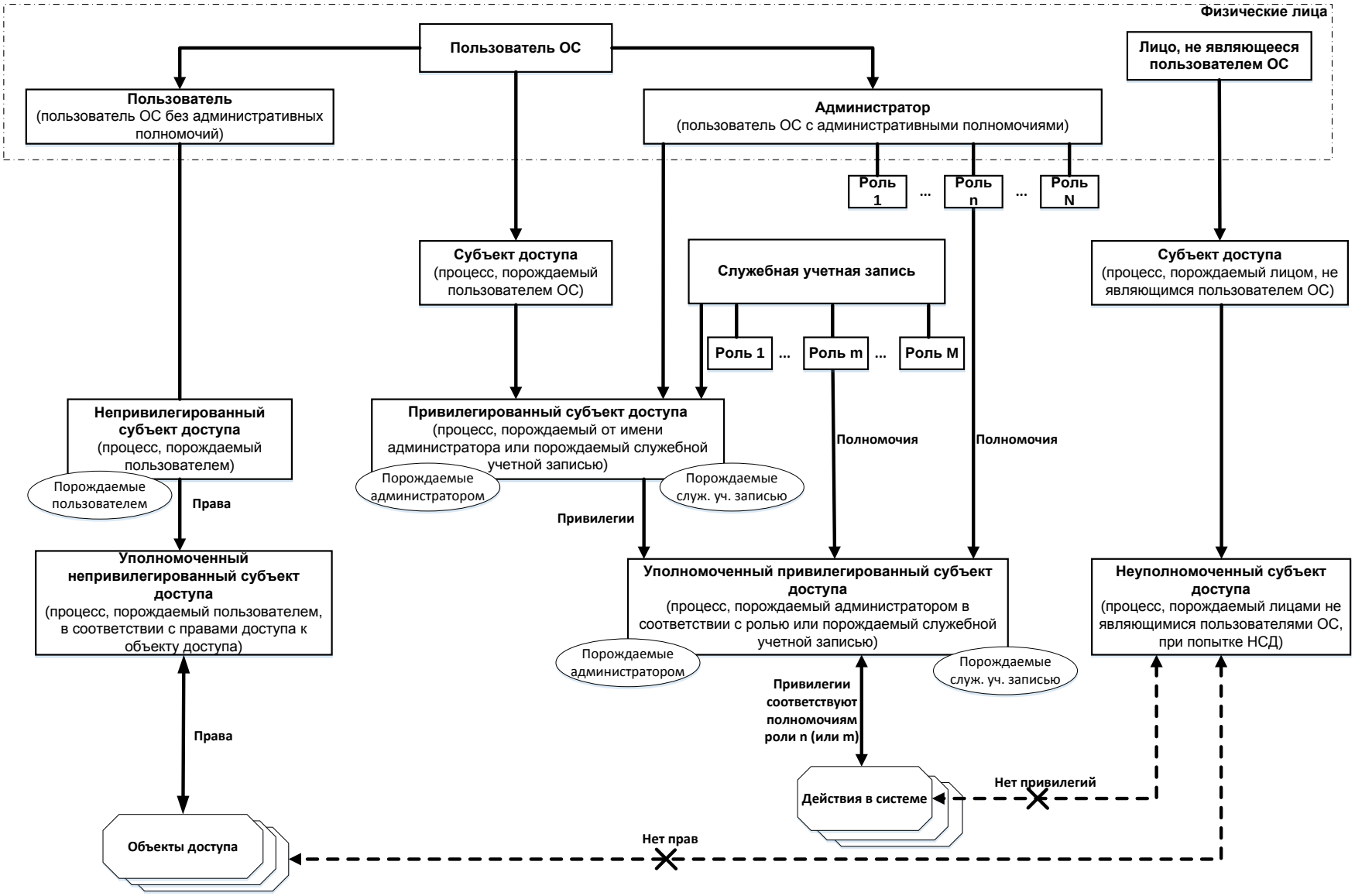

Рисунок 2.1 – Соотношение терминов, применяемых в профиле защиты для обозначения пользователей ОС и субъектов доступа разных категорий

2.2.2. Использование и основные характеристики безопасности объекта оценки

ОО представляет собой программное средство (комплекс программ), реализующее (реализующий) функции защиты от несанкционированного доступа к информации, обрабатываемой на средствах вычислительной техники, находящихся под управлением данного программного средства (комплекса программ).

ОО должен обеспечивать нейтрализацию следующих угроз безопасности информации:

несанкционированный доступ к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен;

ограничение нарушителем доступа пользователей ОС к ресурсам средства вычислительной техники, на котором установлена ОС за счет длительного удержания вычислительного ресурса в загруженном состоянии путем осуществления нарушителем многократных запросов, требующих большого количества времени на их обработку;

недоступность вычислительных ресурсов (процессорное время, оперативная память) для критичных служб ОС и функционирующего прикладного программного обеспечения (приложений) вследствие нерационального распределения ресурсов между потоками служб и приложений (без учета степени их критичности);

несанкционированное или непреднамеренное удаление информации со средства вычислительной техники, функционирующего под управлением ОС;

утечка или несанкционированное изменение информации в оперативной памяти, используемой различными процессами и формируемыми ими потоками данных;

несанкционированное внесение нарушителем изменений в объекты хранения конфигурационных данных, которые влияют на функционирование отдельных сервисов, приложений или ОС в целом;

осуществление восстановления (подбора) аутентификационной информации администраторов и пользователей ОС;

использование нарушителем идентификационной и начальной аутентификационной информации, соответствующей учетной записи пользователя ОС;

несанкционированное внесение изменений в журналы регистрации событий безопасности ОС (журналы аудита);

несанкционированный доступ к информации вследствие использования пользователями неразрешенного программного обеспечения;

несанкционированный доступ субъектов доступа к информации, обработка которой осуществлялась в рамках сеансов (сессий) других субъектов доступа.

В состав ОС как объекта оценки входят следующие компоненты:

загрузчик ОС, обеспечивающий загрузку ядра ОС;

ядро ОС, обеспечивающее управление ресурсами средства вычислительной техники (процессорное время, оперативная память и другие) и выполнение базовых функций по защите информации;

модули уровня ядра (программы, загружаемые ядром ОС и расширяющие его базовые функциональные возможности);

службы ОС, обеспечивающие выполнение функций по обработке и защите информации.

Архитектура безопасности ОС должна обеспечивать:

реализацию монитора обращений, обеспечивающую возможность его исчерпывающего анализа и тестирования;

защищенность монитора обращений (диспетчера доступа) от проникновения (вмешательства), преодоления и обхода;

невозможность доступа субъектов доступа к объектам доступа в обход установленных правил разграничения доступа (управления доступом) в случае сбоя монитора обращений (диспетчера доступа) до восстановления его работоспособности.

В ОС должны быть реализованы следующие функции безопасности:

идентификация и аутентификация;

управление доступом;

регистрация событий безопасности;

ограничение программной среды;

изоляция процессов;

защита памяти;

контроль целостности;

обеспечение надежного функционирования.

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

физическая защита;

доверенная загрузка ОС;

обеспечение условий безопасного функционирования ОС;

обеспечение доверенного маршрута;

обеспечение доверенного канала.

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

В настоящем ПЗ изложены следующие виды требований безопасности, предъявляемые к ОС:

функциональные требования безопасности;

требования доверия к безопасности.

Функциональные требования безопасности ОС, изложенные в ПЗ, включают:

требования к идентификации и аутентификации;

требования к управлению доступом;

требования к регистрации событий безопасности;

требования к ограничению программной среды;

требования к изоляции процессов;

требования к защите памяти;

требования к контролю целостности;

требования к обеспечению надежного функционирования.

Функциональные требования безопасности для ОС 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 ОС типа «В»:

идентификация и аутентификация пользователя до выполнения любых действий по доступу в информационную систему или администратора до выполнения действий по управлению ОС;

возможность задания политики дискреционного и (или) ролевого управления доступом для установленного множества операций, выполняемых субъектами доступа по отношению к объектам доступа;

возможность реализации дискреционного и (или) ролевого управления доступом на основе списков управления доступом (или матрицы управления доступом) и (или) ролей;

возможность установки ПО (компонентов ПО) только администраторами;

контроль запуска компонентов ПО и реагирование на попытки запуска компонентов ПО, произведенные в нарушение установленных правил запуска компонентов ПО;

возможность задания правил автоматического запуска компонентов ПО при загрузке ОС;

контроль целостности компонентов ПО, разрешенного для запуска, и реагирование на попытки запуска компонентов ПО, целостность которых была нарушена;

возможность обеспечения защиты от несогласованностей, возникающих на уровне процессов при параллельной работе с ресурсами средства вычислительной техники и объектами доступа ОС;

возможность блокирования попыток доступа к объектам доступа, если в момент обращения они используются другими процессами;

возможность выполнения определенной задачи системы реального времени в рамках заданных временных ограничений;

защита хранимой аутентификационной информации от неправомерного доступа к ней и раскрытия;

постоянный контроль и проверка правомочности обращений субъектов доступа к объектам доступа;

возможность обеспечения надежных меток времени при проведении аудита безопасности;

возможность обеспечения восстановления штатного режима функционирования ОС;

возможность возврата операционной системы при сбоях и отказах к безопасному состоянию в автоматизированном режиме;

возможность со стороны администратора управлять атрибутами безопасности;

возможность со стороны администратора управлять данными (данными операционной системы), используемыми функциями безопасности ОС;

возможность со стороны администратора управлять выполнением функций безопасности ОС;

возможность со стороны администратора управлять параметрами функций безопасности ОС, данными аудита;

поддержка определенных ролей для ОС и их ассоциация с пользователями ОС;

возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, предоставляемая администратору;

возможность предоставления администратору всей информации аудита в понятном для него виде;

возможность защиты хранимых записей регистрации событий безопасности ОС (аудита) от несанкционированного удаления и предотвращения модификации записей аудита;

возможность выполнения действий, направленных на сохранение данных журнала регистрации событий безопасности ОС и обеспечивающих непрерывность процесса аудита, если журнал регистрации событий безопасности ОС превысит определенный администратором размер;

возможность регистрации возникновения событий, которые в соответствии с ГОСТ Р ИСО/МЭК 15408-2 включены в минимальный уровень аудита.

Требования доверия к безопасности ОС 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 ОС образуют оценочный уровень доверия 1 (ОУД1), усиленный компонентами ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS.1 «Базовый проект» и расширенный компонентами ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы» и AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы».

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

2.2.3. Тип объекта оценки

ОО является ОС типа «В».

ОС типа «В» – это ОС, предназначенная для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

2.2.4. 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 ОО, не рассматриваются.

2.3. Соглашения

Национальные стандарты Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» допускают 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 (присвоенное) 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 ОС.

3. Утверждение о соответствии

3.1. Утверждение о соответствии ГОСТ Р ИСО/МЭК 15408

Настоящий ПЗ 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 национальными стандартами 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 операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы» и AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы», FDP_RSI_EXT.1 «Управление установкой программного обеспечения», FDP_RSP_EXT.1 «Правила запуска компонентов программного обеспечения», FDP_RSP_EXT.2 «Контроль запуска компонентов программного обеспечения», FPO_DFS_EXT.1 «Изоляция процессов», FPO_OBF_EXT.1 «Блокирование файлов процессами», FPO_RIP_EXT.1 «Безопасное выделение областей оперативной памяти», FPO_RTM_EXT.1 «Обеспечение выполнения задачи в интервал времени», FPT_MTR_EXT.1 «Монитор обращений», FPT_APW_EXT.1 «Защита хранимой аутентификационной информации», FRU_PRS_EXT.3 «Приоритизация процессов»).

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), усиленный компонентами ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS.1 «Базовый проект» и расширенный компонентами ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на

безопасность операционной системы» и AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы».

3.4. Обоснование соответствия

Включение функциональных требований и требований доверия к ОС в настоящий ПЗ определяется Требованиями безопасности информации к операционным системам, утвержденными приказом ФСТЭК России от 19 августа 2016 г. № 119.

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 настоящему ПЗ и другому (другим) ПЗ.

4. Цели безопасности

4.1. Цели безопасности для среды функционирования

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

Цель для среды функционирования ОО-1

Совместимость

ОО должен быть совместим с СВТ (ИС), в котором (которой) он функционирует.

Цель для среды функционирования ОО-2

Эксплуатация ОО

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

Цель для среды функционирования ОО-3

Физическая защита ОО

Должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует ОО.

Цель для среды функционирования ОО-4

Доверенная загрузка ОС

Должна быть обеспечена доверенная загрузка ОС (блокирование попыток несанкционированной загрузки, контроль доступа субъектов доступа к процессу загрузки, контроль целостности компонентов загружаемой операционной среды).

Цель для среды функционирования ОО-5

Обеспечение условий безопасного функционирования

Должны быть обеспечены необходимые ресурсы для выполнения функциональных возможностей безопасности операционной системы, хранения резервных копий, создаваемых операционной системой, а также защищенное хранение данных операционной системы и защищаемой информации.

Цель для среды функционирования ОО-6

Контроль установки программного обеспечения

Должно быть обеспечено ограничение на установку программного обеспечения и его компонентов, не задействованных в технологическом процессе обработки информации.

Цель для среды функционирования ОО-7

Доверенный маршрут

Должен обеспечиваться доверенный маршрут между ОС и пользователями ОС (администраторами, пользователями).

Цель для среды функционирования ОО-8

Доверенный канал

Должен обеспечиваться доверенный канал передачи данных между ОС и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование.

Цель для среды функционирования ОО-9

Защита от отключения

Должна быть обеспечена невозможность отключения (обхода) компонентов ОС.

Цель для среды функционирования ОО-10

Ограничение несанкционированного копирования информации, содержащейся в ОС

Должны быть реализованы меры, препятствующие несанкционированному копированию информации, содержащейся в ОС, на съемные машинные носители информации (или в другое место вне информационной системы).

В том числе должен осуществляться контроль вноса (выноса) в (из) контролируемую зону (контролируемой зоны) съемных машинных носителей информации.

Цель для среды функционирования ОО-11

Проверка устанавливаемых внешних модулей уровня ядра

Должна быть осуществлена проверка целостности внешних модулей уровня ядра, получаемых от заявителя (разработчика, производителя), перед их установкой в операционную систему.

Цель для среды функционирования ОО-12

Приоритизация процессов

Должно быть обеспечено выделение вычислительных ресурсов для процессов и (или) формируемых ими потоков данных в соответствии с их приоритетами.

Цель для среды функционирования ОО-13

Требования к персоналу-1

Лица, ответственные за эксплуатацию ОО, должны обеспечивать функционирование ОО, в точности руководствуясь эксплуатационной документацией.

Цель для среды функционирования ОО-14

Требования к персоналу-2

Лица, ответственные за эксплуатацию ОО, должны обеспечить, чтобы аутентификационная информация для каждой учетной записи пользователя ОС содержались в тайне и были недоступны лицам, не уполномоченным использовать данную учетную запись.

Цель для среды функционирования ОО-15

Генерация аутентификационной информации

Должна обеспечиваться возможность генерации (определения) аутентификационной информации с метрикой качества, обеспечивающей стойкость по отношению к нарушителю с базовым потенциалом нападения.

5. Определение расширенных компонентов

В данном разделе ПЗ представлены расширенные компоненты для ОС.

5.1. Определение расширенных (специальных) компонентов функциональных требований безопасности объекта оценки

Для ОО 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).

Компоненты функциональных требований безопасности, сформулированные в явном виде, представлены в приложении А к настоящему профилю защиты.

5.2. Определение расширенных (специальных) компонентов требований доверия к безопасности объекта оценки

Для ОО определены следующие расширенные (специальные) компоненты требований доверия к безопасности: ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы», AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы», 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».

Компоненты требований доверия к безопасности, сформулированные в явном виде, представлены в приложении Б к настоящему профилю защиты.

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 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 ОУД1, расширенного компонентами ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы», и AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы» сформулированными 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_SEL.1	Избирательный аудит
FAU_SAR.1	Просмотр аудита
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_RSI_EXT.1	Управление установкой программного обеспечения
FDP_RSP_EXT.1	Правила запуска компонентов программного обеспечения
FDP_RSP_EXT.2	Контроль запуска компонентов программного обеспечения
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MTD.1	Управление данными функций безопасности
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
FPT_MTR_EXT.1	Монитор обращений
FPT_APW_EXT.1	Защита хранимой аутентификационной информации
FPT_RCV.1	Ручное восстановление
FPT_STM.1	Надежные метки времени
FPO_DFS_EXT.1	Изоляция процессов
FPO_OBF_EXT.1	Блокирование файлов процессами
FRU_PRS_EXT.3	Приоритизация процессов

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) [события, приведенные во втором столбце таблицы 6.2, а также [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 доступа (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*].

Таблица 6.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FMT_MOF.1	Все модификации политики аудита	
FMT_MTD.1	Все модификации аутентификационной информации	Смена значений аутентификационной информации
FPO_DFS_EXT.1	Сбои в работе механизма изоляции процессов	

Зависимости: FPT_STM.1 Надежные метки времени.

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [назначение: ***роли администраторов в соответствии с FMT_SMR.1***] возможность читать [назначение: *список информации аудита*] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **администратору** 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, потенциально подвергаемых аудиту, базируясь на следующих атрибутах:
а) *идентификатор объекта доступа, идентификатор субъекта доступа*, [выбор: *идентификатор пользователя ОС, 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.

FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.1.1 ФБО должны защищать хранимые записи аудита в журнале **регистрации событий безопасности ОС** от несанкционированного удаления.

FAU_STG.1.2 ФБО должны быть способны [выбор, (выбрать одно из): *предотвращать, выявлять*] несанкционированную модификацию хранимых записей аудита в журнале **регистрации событий безопасности ОС**.

Зависимости: FAU_GEN.1 Генерация данных аудита.

FAU_STG.3 Действия в случае возможной потери данных аудита

FAU_STG.3.1 ФБО должны выполнить [назначение: *действия, которые нужно предпринять в случае возможного сбоя хранения журнала **регистрации событий безопасности ОС***], если журнал **регистрации событий безопасности ОС** превышает [назначение: *принятое ограничение*].

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита.

6.1.2. Защита данных пользователя (FDP)

FDP_ACC.1(1) Ограниченное управление доступом

FDP_ACC.1.1(1) ФБО должны осуществлять [политику дискреционного управления доступом] для [назначение: *список субъектов **доступа** и объектов **доступа***].

Зависимости: FDP_ACF.1(1) Управление доступом, основанное на атрибутах безопасности.

Замечания по применению: компонент FDP_ACC.1(1) включается в ЗБ, если в Политике безопасности-2 и Цели безопасности-2 определена реализация дискреционного метода управления доступом.

FDP_ACC.1(2) Ограниченное управление доступом

FDP_ACC.1.1(2) ФБО должны осуществлять [политику ролевого управления доступом] для [назначение: *список ролей и объектов*].

Зависимости: FDP_ACF.1(2) Управление доступом, основанное на атрибутах безопасности.

Замечания по применению: компонент FDP_ACC.1(2) включается в ЗБ, если в Политике безопасности-2 и Цели безопасности-2 определена реализация ролевого метода управления доступом.

FDP_ACF.1(1) Управление доступом, основанное на атрибутах безопасности (дискреционное управление доступом к объектам ОС)

FDP_ACF.1.1(1) ФБО должны осуществлять [политику дискреционного управления доступом] к объектам, основываясь на [назначение: *список **доступа** и объектов **доступа**, находящихся под управлением **политики дискреционного управления доступом**, и для каждого из них – относящиеся к **политике дискреционного управления доступом** атрибуты безопасности или именованные группы атрибутов безопасности*].

FDP_ACF.1.2(1) ФБО должны осуществлять следующие правила определения того, разрешена ли операция управляемого субъекта **доступа** на управляемом объекте **доступа**: [назначение: *правила управления доступом управляемых субъектов **доступа** к управляемым объектам **доступа** с использованием управляемых операций на них, **основанные на списках контроля доступа***].

FDP_ACF.1.3(1) ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: [нет].

FDP_ACF.1.4(1) ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах: [назначение: *правила, основанные на атрибутах безопасности, которые явно запрещают доступ субъектов **доступа** к объектам **доступа***].

Зависимости: FDP_ACC.1(1) Ограниченное управление доступом; FMT_MSA.3 Инициализация статических атрибутов.

Замечания по применению: компонент FDP_ACF.1(1) включается в ЗБ, если в Политике безопасности-2 и Цели безопасности-2 определена реализация дискреционного метода управления доступом.

FDP_ACF.1(2) Управление доступом, основанное на атрибутах безопасности (ролевое управление доступом к объектам ОС)

FDP_ACF.1.1(2) ФБО должны осуществлять [политику ролевого управления доступом] к объектам, основываясь на [назначение: *список ролей и объектов, находящихся под управлением **политики ролевого управления доступом**, и для каждого из них – относящиеся к **политике ролевого управления доступом** атрибуты безопасности или именованные группы атрибутов безопасности*].

FDP_ACF.1.2(2) ФБО должны осуществлять следующие правила определения того, разрешена ли операция управляемого субъекта **доступа** на управляемом объекте: [назначение: *правила управления доступом управляемых ролей к управляемым объектам с использованием управляемых операций на них,* ***основанные на списках прав доступа***].

FDP_ACF.1.3(2) ФБО должны явно разрешать доступ субъектов **доступа** к объектам **доступа**, основываясь на следующих дополнительных правилах: [нет].

FDP_ACF.1.4(2) ФБО должны явно отказывать в доступе субъектов **доступа** к объектам **доступа**, основываясь на следующих дополнительных правилах: [назначение: *правила, основанные на атрибутах безопасности, которые явно запрещают доступ ролей к объектам*].

Зависимости: FDP_ACC.1(2) Ограниченное управление доступом; FMT_MSA.3 Инициализация статических атрибутов.

Замечания по применению: компонент FDP_ACF.1(2) включается в ЗБ, если в Политике безопасности-2 и Цели безопасности-2 определена реализация ролевого метода управления доступом.

FDP_RSI_EXT.1 Управление установкой программного обеспечения

FDP_RSI_EXT.1.1 Функциональные возможности безопасности операционной системы должны предоставлять возможность установки (инсталляции) программного обеспечения (компонентов программного обеспечения) только [назначение: ***роли пользователей ОС в соответствии с FMT_SMR.1***].

Зависимости: отсутствуют.

FDP_RSP_EXT.1 Правила контроля запуска компонентов программного обеспечения

FDP_RSP_EXT.1.1 Функциональные возможности безопасности операционной системы должны обеспечивать возможность задания перечня компонентов программного обеспечения, *разрешенных для автоматического запуска при загрузке операционной системы, запрещенных для автоматического запуска при загрузке операционной системы*, [выбор: *разрешенных для запуска в процессе функционирования операционной системы; запрещенных для запуска в процессе функционирования операционной системы*].

Зависимости: отсутствуют.

FDP_RSP_EXT.2 Контроль запуска компонентов программного обеспечения

FDP_RSP_EXT.2.1 Функциональные возможности безопасности операционной системы должны контролировать запуск компонентов программного обеспечения и при обнаружении попытки запуска компонентов программного обеспечения, произведенных в нарушение установленных правил запуска компонентов программного обеспечения, **обеспечивать** [выбор: *оповещение пользователя, выполняющего запуск, и администратора,* [назначение: *иные действия*]], *блокирование попытки запуска*.

FDP_RSP_EXT.2.2 Функциональные возможности безопасности операционной системы должны контролировать целостность компонентов программного обеспечения, разрешенного для запуска, и при обнаружении попытки запуска компонентов программного обеспечения, целостность которых была нарушена, **обеспечивать возможность** [выбор: *оповещение пользователя, выполняющего запуск, и администратора,* [назначение: *иные действия*]], *блокирование попытки запуска*.

Зависимости: отсутствуют.

Замечания по применению:

1. В FDP_RSP_EXT.2.1 разработчику ЗБ следует определить типы пользователей ОС, для которых реализованы функциональные возможности по оповещению о попытках запуска компонентов программного обеспечения, произведенных в нарушение установленных правил запуска компонентов программного обеспечения.

Для информирования администратора о попытках запуска компонентов программного обеспечения, произведенных в нарушение установленных правил запуска компонентов программного обеспечения, в FAU_GEN.1 необходимо предусмотреть действия по аудиту.

2. В FDP_RSP_EXT.2.2 разработчику ЗБ следует определить типы пользователей ОС, для которых реализованы функциональные возможности по оповещению о попытках запуска компонентов программного обеспечения, целостность которых была нарушена.

Для информирования администратора о попытках запуска компонентов программного обеспечения, целостность которых была нарушена, в FAU_GEN.1 необходимо предусмотреть действия по аудиту.

6.1.3. Идентификация и аутентификация (FIA)

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый пользователь **ОС** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя **ОС**.

Зависимости: FIA_UID.1 Выбор момента идентификации.

FIA_UID.2 Идентификация до любых действий пользователя

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

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.

Замечания по применению:

1. Объект оценки не должен содержать функциональных возможностей безопасности, атрибутов безопасности ФБО, параметров ФБО, данных ФБО, настроек, ролей и иных сущностей, связанных с функциями управления, доступных заявителю (разработчику, производителю) ОО, но недоступных потребителю ОО для контроля и изменения.

2. Объект оценки не должен содержать настроек (преднастроек) функциональных возможностей безопасности, атрибутов безопасности ФБО, параметров ФБО, данных ФБО и иных сущностей, настраиваемых при производстве, установленных заявителем (разработчиком, производителем) ОО, недоступных потребителю ОО для контроля и изменения и не описанных в документации на ОО.

3. В ЗБ должны быть описаны все возможности по управлению для каждой ФБО, в том числе все управляемые сущности (механизмы, интерфейсы, правила, каналы и т.д.), способы администрирования ОО (локальное, удаленное), уполномоченные идентифицированные роли (администраторы, пользователи), которым предоставлены возможности по управлению, а для неиспользуемых возможностей по управлению ФБО должно быть представлено соответствующее обоснование.

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 [назначение: ***роли администраторов в соответствии с FMT_SMR.1***].

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

Замечания по применению:

1. Объект оценки не должен содержать данных ФБО, доступных заявителю (разработчику, производителю) ОО, но недоступных потребителю ОО для контроля и изменения.

2. Объект оценки не должен содержать настроек (преднастроек) данных ФБО, установленных заявителем (разработчиком, производителем) ОО, недоступных потребителю ОО для контроля и изменения и не описанных в документации на ОО.

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 [администратору].

Зависимости: FMT_SMR.1 Роли безопасности.

Замечания по применению:

1. Объект оценки не должен содержать функций безопасности, доступных заявителю (разработчику, производителю) ОО, но недоступных потребителю ОО для контроля и изменения.

2. Объект оценки не должен содержать настроек (преднастроек) функций безопасности, установленных заявителем (разработчиком, производителем) ОО, недоступных потребителю ОО для контроля и изменения и не описанных в документации на ОО.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли **пользователей ОС**:

[

а) администратор [назначение: *роли администраторов*];

б) пользователь

].

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

Зависимости: FIA_UID.1 Выбор момента идентификации.

Замечание по применению: объект оценки не должен поддерживать роли пользователей ОС, доступные заявителю (разработчику, производителю) ОО, но недоступные потребителю ОО для контроля и изменения.

FMT_MSA.1(1) Управление атрибутами безопасности

FMT_MSA.1.1(1) ФБО должны осуществлять [выбор: *ролевая политика управления*, [назначение: ***иная политика управления***]], предоставляющую возможность [выбор: *изменять значения по умолчанию, запрашивать, модифицировать, удалять*, [назначение: *другие операции*]] атрибуты безопасности [назначение: *список атрибутов безопасности*] только [администратору].

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

Замечания по применению: компонент предназначен для обеспечения возможности управления атрибутами безопасности (права доступа, типы доступа и иные атрибуты) для осуществления политики дискреционного управления доступом (при использовании дискреционного метода управления доступом).

FMT_MSA.1(2) Управление атрибутами безопасности

FMT_MSA.1.1(2) ФБО должны осуществлять [выбор: *ролевая политика управления*, [назначение: ***иная политика управления***]], предоставляющую возможность [выбор: *изменять значения по умолчанию, запрашивать, модифицировать, удалять,* [назначение*: другие операции*]] атрибуты безопасности [назначение: *список атрибутов безопасности*] только [администратору].

Зависимости: [FDP_ACC.1(2) Ограниченное управление доступом или FDP_IFC.1 Ограниченное управление информационными потоками];
FMT_SMR.1 Роли безопасности;
FMT_SMF.1 Спецификация функций управления.

Замечания по применению:

1. Компонент предназначен для обеспечения возможности управления атрибутами безопасности для осуществления политики ролевого управления доступом (при использовании ролевого метода управления доступом).

2. Объект оценки не должен содержать атрибутов безопасности ФБО, доступных заявителю (разработчику, производителю) ОО, но недоступных потребителю ОО для контроля и изменения.

3. Объект оценки не должен содержать настроек (преднастроек) атрибутов безопасности ФБО, установленных заявителем (разработчиком, производителем) ОО, недоступных потребителю ОО для контроля и изменения и не описанных в документации на ОО.

6.1.5. Защита ФБО (FPT)

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБО должны быть способны предоставлять надежные метки времени.

Зависимости: отсутствуют.

FPT_RCV.1 Ручное восстановление

FPT_RCV.1.1 После [сбоя или прерывания обслуживания] ФБО должны перейти в режим аварийной поддержки, который предоставляет возможность возврата ОС к безопасному состоянию.

Зависимости: AGD_OPE.1 Руководство пользователя по эксплуатации.

FPT_APW_EXT.1 Защита хранимой аутентификационной информации

FPT_APW_EXT.1.1 Функциональные возможности безопасности должны предотвращать хранение аутентификационной информации в открытом виде.

FPT_APW_EXT.1.2 Функциональные возможности безопасности должны предотвращать чтение **хранимой** аутентификационной информации в открытом виде.

Зависимости: отсутствуют.

FPT_MTR_EXT.1 Монитор обращений

FPT_MTR_EXT.1.1 Функциональные возможности безопасности операционной системы должны осуществлять постоянный контроль обращений *субъектов доступа к объектам доступа*, [выбор: *субъектов доступа к информации,* [назначение: *иные типы обращений*]**, нет**].

FPT_MTR_EXT.1.2 Функциональные возможности безопасности операционной системы должны осуществлять проверку правомочности обращений к информации на основе установленных политик [выбор: *политика управления доступом*].

FPT_MTR_EXT.1.3 Функциональные возможности безопасности операционной системы должны отклонять или удовлетворять обращения на доступ к информации по результатам проверки их правомочности.

Зависимости: отсутствуют.

Замечания по применению:

1. В FPT_MTR_EXT.1.1 разработчик ЗБ может дополнительно к типу обращений «субъектов доступа к объектам доступа» определить иные типы обращений, контролируемых ОС. Если ОС осуществляет контроль обращений только «субъектов доступа к объектам доступа», то «выбор» в FPT_MTR_EXT.1.1 может быть выполнен как «нет».

2. В FPT_MTR_EXT.1.2 разработчик ЗБ устанавливает: дискреционную и (или) ролевую политику управления доступом; также может быть установлена мандатная политика управления доступом.

6.1.6. Функциональные возможности безопасности операционной системы (FPO)

FPO_DFS_EXT.1 Изоляция процессов

FPO_DFS_EXT.1.1 Функциональные возможности безопасности операционной системы должны обеспечивать защиту от несогласованностей (противоречивости), возникающих на уровне процессов, при параллельной работе со следующими объектами: *области памяти, файлы*, [выбор: *устройства,* [назначение: *другие объекты*]**, нет**].

FPO_DFS_EXT.1.2 Функциональные возможности безопасности операционной системы должны обеспечивать возможность реализации следующих процедур для изоляции параллельных процессов [выбор: *изоляцию процессов в оперативной памяти, управление временем использования процессами общих ресурсов, именование процессов, предоставление процессу виртуального адресного пространства*, [назначение: *иные процедуры*]].

Зависимости: отсутствуют.

Замечания по применению:

При изоляции процесса в оперативной памяти другие процессы не должны иметь доступ к области памяти, выделенной для данного процесса. Все потоки, формируемые процессом, также должны использовать только выделенное для соответствующего процесса адресное пространство. Для взаимодействия изолированных процессов должны применяться специальные интерфейсы процессов.

Управление временем использования процессами общих ресурсов позволяет использовать общие ресурсы (такие как процессор) несколькими процессами или потоками данных одновременно. Для каждого процесса выделяются установленные промежутки времени (длительность таких промежутков зависит от приоритета процесса), в течение которых процесс может использовать общий ресурс.

Именование процессов предусматривает идентификацию процессов с использованием уникальных идентификаторов. Идентификация процессов необходима для обеспечения возможности операционной системы управлять процессами, а также для обеспечения возможности взаимодействия процессов друг с другом.

Предоставление процессу виртуального адресного пространства необходимо для того, чтобы процесс воспринимал все выделенные ему области оперативной памяти как единое адресное пространство и не осуществлял прямых обращений к физической памяти.

FPO_OBF_EXT.1 Блокирование файлов процессами

FPO_OBF_EXT.1.1 Функциональные возможности безопасности операционной системы должны блокировать попытки выполнения следующих операций: *удаление*, [выбор: *модификация, [назначение: иные операции]*, **нет**] над файлами, если в момент обращения к файлу **субъекта доступа (процесса)** он используется другим **субъектом доступа (**процессом**)**.

Зависимости: отсутствуют.

6.1.7. Использование ресурсов (FRU)

FRU_PRS_EXT.3 Приоритизация процессов

FRU_PRS_EXT.3.1 Функциональные возможности безопасности операционной системы должны осуществлять приоритизацию процессов на основе установленных приоритетов значений атрибутов процессов [назначение: *атрибуты процессов, используемые для приоритизации*] и заданной функции определения приоритета процесса на основе приоритетов значений атрибутов процесса.

FRU_PRS_EXT.3.2 Функциональные возможности безопасности операционной системы должны обеспечить выполнение процессов [назначение: *типы процессов*] и (или) доступ к вычислительным ресурсам на основе приоритизации процессов.

Зависимости: FMT_MSA.1 Управление атрибутами безопасности;
FMT_MTD.1 Управление данными функциональных возможностей безопасности.

6.2. 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 ОУД1, усиленный компонентами ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS.1 «Базовый проект» и расширенный компонентами ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы» и AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы» (см. таблицу 6.6).

Таблица 6.6 – Требования доверия к безопасности ОО

Классы доверия	**Идентификаторы компонентов доверия**	**Названия компонентов доверия**
Разработка	ADV_FSP.5	Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках
	ADV_TDS.1	Базовый проект
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
	ALC_FPU_EXT.1	Процедуры обновления программного обеспечения ОС
	ALC_LCD_EXT.3	Определенные разработчиком сроки поддержки
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 ОС	ALC_FPU_EXT.1	Процедуры обновления программного обеспечения ОС
Обновление ОС	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность операционной системы

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
	AMA_SIA_EXT.6	Анализ влияния внешних модулей уровня ядра на безопасность операционной системы

6.2.1. Разработка (ADV)

ADV_FSP.5 Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках

Зависимости: ADV_TDS.1 Базовый проект;
ADV_IMP.1 Представление реализации ФБО.

Элементы действий заявителя (разработчика, производителя)

ADV_FSP.5.1D Заявитель (разработчик, производитель) должен представить функциональную спецификацию.

ADV_FSP.5.2D Заявитель (разработчик, производитель) должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления документированных материалов

ADV_FSP.5.1C В функциональной спецификации должны быть полностью представлены ФБО.

ADV_FSP.5.2C Функциональная спецификация должна содержать полуформальное описание ИФБО.

ADV_FSP.5.3C В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV_FSP.5.4C В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV_FSP.5.5C В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.

ADV_FSP.5.6C Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.

ADV_FSP.5.7C Функциональная спецификация должна содержать описание всех сообщений об ошибках, возникающих не в результате вызова ИФБО.

ADV_FSP.5.8C Функциональная спецификация должна содержать обоснование каждого сообщения об ошибке, содержащегося в реализации ФБО, но не являющегося результатом вызова ИФБО.

ADV_FSP.5.9C В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий испытательной лаборатории

ADV_FSP.5.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.5.2E 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 10.4.5 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ADV_TDS.1 Базовый проект

Зависимости: ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации

Элементы действий заявителя (разработчика, производителя)

ADV_TDS.1.1D Разработчик должен представить проект ОО.

ADV_TDS.1.2D Разработчик должен обеспечить прослеживание от ИФБО в функциональной спецификации к самому низкому уровню декомпозиции, имеющемуся в проекте ОО.

Элементы содержания и представления документированных материалов

ADV_TDS.1.1C В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV_TDS.1.2C В проекте должны быть идентифицированы все подсистемы ФБО.

ADV_TDS.1.3C В проекте должно приводиться описание режима функционирования для каждой подсистемы, поддерживающей выполнение ФТБ или не влияющей на их выполнение, с предоставлением детальной информации, достаточной для того, чтобы установить, что подсистема не является осуществляющей выполнение ФТБ.

ADV_TDS.1.4C В проекте должна приводиться аннотация осуществляющих выполнение ФТБ режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.

ADV_TDS.1.5C В проекте должно приводиться описание взаимодействий между осуществляющими выполнение ФТБ подсистемами ФБО, а также между ними и другими подсистемами ФБО.

ADV_TDS.1.6C В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий испытательной лаборатории

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

ADV_TDS.1.2E Испытательная лаборатория должна сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

6.2.2. 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 уместных предупреждений.

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

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

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

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

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

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

Элементы действий испытательной лаборатории

AGD_OPE1.1E Испытательная лаборатория должна подтвердить, что 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 ОС, 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 ОС – 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».

6.2.3. 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».

ALC_FPU_EXT.1 Процедуры обновления программного обеспечения операционной системы

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_FPU_EXT.1.1D Заявитель (разработчик, производитель) должен разработать и реализовать технологию обновления ОС для [выбор: *обновление, направленное на устранение уязвимостей ОС; иное обновление, оказывающее влияние на безопасность ОС; обновление, не оказывающее влияния на безопасность ОС*].

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

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

ALC_FPU_EXT.1.4D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру предоставления обновлений потребителям ОС, 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 ОС должна содержать описание технологии выпуска обновлений ОС.

ALC_FPU_EXT.1.2C Документация ОС должна содержать регламент обновления ОС, 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 ОС 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.

ALC_LCD_EXT.3 Определенные разработчиком сроки поддержки

Зависимости: отсутствуют.

Элементы действий (разработчика, производителя)

ALC_LCD_EXT.3.1D Заявитель, разработчик, производитель должны установить в совместной декларации срок [назначение: *срок*], в течение которого они обязуются выполнять все необходимые действия по поддержке ОО, направленные на обеспечение поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2D Заявитель, разработчик, производитель должны обеспечить представление совместной декларации о сроке поддержки ОО вместе с заявкой на сертификацию ОО.

Элементы содержания и представления документированных материалов

ALC_LCD_EXT.3.1C Декларация о сроке поддержки ОО должна содержать план поддержки ОО на весь задекларированный срок, включающий описание всех предпринимаемых действий по обеспечению поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2C Декларация о сроке поддержки ОО должна содержать сведения о поддерживаемой версии ОО.

Элементы действий испытательной лаборатории

ALC_LCD_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 ALC_LCD_EXT.3.1C и ALC_LCD_EXT.3.2C.

6.2.4. 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 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 **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.

6.2.5. 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 ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

6.2.6. 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 представить ОО для тестирования.

Элементы содержания и представления документированных материалов

AVA_VAN.1.1C ОО должен быть пригоден для тестирования.

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».

6.2.7. Требования к объекту оценки, сформулированные в явном виде

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность операционные системы

Элементы действий заявителя

AMA_SIA_EXT.3.1D Заявитель должен представить материалы анализа влияния обновлений на безопасность ОС.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность ОС должны содержать краткое описание влияния обновлений на задание по безопасности, **реализацию ОС 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 ОС**.

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

Элементы действий испытательной лаборатории

AMA_SIA_EXT.3.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению документированных материалов, 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 ОС.

AMA_SIA_EXT.6 Анализ влияния внешних модулей уровня ядра на безопасность операционной системы

Элементы действий заявителя

AMA_SIA_EXT.6.1D Разработчик (заявитель, производитель) должен предоставлять в испытательную лабораторию материалы анализа влияния модулей уровня ядра на безопасность ОС и комплект идентифицированных (промаркированных) внешних модулей уровня ядра.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.6.1C Материалы анализа влияния внешних модулей уровня ядра на безопасность ОС должны содержать краткое описание влияния модулей уровня ядра на задание по безопасности и функции безопасности ОС или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.6.2C Материалы анализа **влияния** модулей уровня ядра ОС на безопасность ОС, должны идентифицировать функции безопасности и компоненты операционной системы, на которые влияют внешние модули ядра ОС.

Элементы действий испытательной лаборатории

AMA_SIA_EXT.6.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению документированных материалов.

AMA_SIA_EXT.6.2E Испытательная лаборатория должна подтвердить влияние (отсутствие влияния) модулей уровня ядра на безопасность ОС.

Приложение А

Расширенные (специальные) компоненты функциональных требований безопасности объекта оценки

Для ОО 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).

А.1. Класс FPO «Функциональные возможности безопасности операционной системы»

А.1.1. Изоляция процессов (FPO_DFS_EXT)

Характеристика семейства

Семейство FPO_DFS_EXT «Изоляция процессов» определяет компоненты требований, направленные на обеспечение операционной системой изоляции процессов для защиты от возможных несогласованностей (противоречивости) при параллельной работе с объектами доступа.

Ранжирование компонентов

FPO_DFS_EXT.1 «Изоляция процессов» предназначен для задания требований, связанных с обеспечением объектом оценки защиты от несогласованностей (противоречивости), возникающих на уровне процессов, при параллельной работе с объектами доступа, путем реализации определенных процедур (изоляцию процессов в оперативной памяти, управление временем использования процессами общих ресурсов, именование процессов, предоставление процессу виртуального адресного пространства, и иных процедур).

Управление: FPO_DFS_EXT.1

Действия по управлению не определены.

Аудит: FPO_DFS_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPO_DFS_EXT.1 Изоляция процессов

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPO_DFS_EXT.1.1

Функциональные возможности безопасности операционной системы должны обеспечивать защиту от несогласованностей (противоречивости), возникающих на уровне процессов при параллельной работе со следующими объектами [выбор: *области памяти, файлы, устройства* [назначение: *другие объекты*]].

FPO_DFS_EXT.1.2

Функциональные возможности безопасности операционной системы должны обеспечивать возможность реализации следующих процедур для изоляции параллельных процессов [выбор: *изоляцию процессов в оперативной памяти, управление временем использования процессами общих ресурсов, именование процессов, предоставление процессу виртуального адресного пространства,* [назначение: *иные процедуры*]].

А.1.2. Блокирование файлов процессами (FPO_OBF_EXT)

Характеристика семейства

Семейство FPO_OBF_EXT «Блокирование файлов процессами» определяет компоненты требований, направленные на обеспечение операционной системой невозможности выполнения операций над файлами при их использовании другими процессами.

Ранжирование компонентов

FPO_OBF_EXT.1 «Блокирование файлов процессами» предназначен для задания требований, связанных с тем, чтобы объект оценки обеспечивал блокирование выполнения операций над файлами при их использовании другими процессами.

Управление: FPO_OBF_EXT.1

Действия по управлению не определены.

Аудит: FPO_OBF_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPO_OBF_EXT.1 Блокирование файлов процессами

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPO_OBF_EXT.1.1

Функциональные возможности безопасности операционной системы должны предоставлять возможность блокирования попытки выполнения следующих операций [выбор: *модификация, удаление*] над файлами, если в момент обращения к файлу он используется другим процессом.

А.2. Класс FDP «Защита данных пользователя операционной системы»

А.2.1. Управление установкой программного обеспечения (FDP_RSI_EXT)

Характеристика семейства

Семейство FDP_RSI_EXT «Управление установкой программного обеспечения» определяет компоненты требований, направленные на предотвращение несанкционированной установки программного обеспечения (компонентов программного обеспечения).

Ранжирование компонентов

FDP_RSI_EXT.1 «Управление установкой программного обеспечения» предназначен для задания требований по обеспечению возможности установки программного обеспечения (компонентов программного обеспечения) только уполномоченными субъектами.

Управление: FDP_RSI_EXT.1

Действия по управлению не определены

Аудит: FDP_RSI_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FDP_RSI_EXT.1 Управление установкой программного обеспечения

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FDP_RSI_EXT.1.1

Функциональные возможности безопасности операционной системы должны предоставлять возможность установки (инсталляции) программного обеспечения (компонентов программного обеспечения) только уполномоченными субъектами [назначение: *уполномоченные идентифицированные роли*].

А.2.2. Управление запуском компонентов программного обеспечения (FDP_RSP_EXT)

Характеристика семейства

Семейство FDP_RSP_EXT «Управление запуском компонентов программного обеспечения» определяет компоненты требований, связанные с контролем запуска компонентов программного обеспечения.

Ранжирование компонентов

FDP_RSP_EXT.1 «Правила запуска компонентов программного обеспечения» предназначен для задания требований по ведению перечня компонентов программного обеспечения, разрешенных и (или) запрещенных для запуска.

FDP_RSP_EXT.2 «Контроль запуска компонентов программного обеспечения» предназначен для задания требований, связанных с осуществлением контроля запуска компонентов программного обеспечения и выполнения заданных действий при нарушении правил запуска компонентов программного обеспечения.

Управление: FDP_RSP_EXT.1, FDP_RSP_EXT.2

Действия по управлению не определены.

Аудит: FDP_RSP_EXT.1, FDP_RSP_EXT.2

Действия или события, подвергаемые аудиту, не определены.

FDP_RSP_EXT.1 Правила контроля запуска компонентов программного обеспечения

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FDP_RSP_EXT.1.1

Функциональные возможности безопасности операционной системы должны обеспечивать возможность задания перечня компонентов программного обеспечения, [выбор: ***разрешенных для автоматического запуска при загрузке операционной системы; запрещенных для автоматического запуска при загрузке операционной системы; разрешенных для запуска в процессе функционирования операционной системы; запрещенных для запуска в процессе функционирования операционной системы*****].**

FDP_RSP_EXT.2 Контроль запуска компонентов программного обеспечения

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FDP_RSP_EXT.2.1

Функциональные возможности безопасности операционной системы должны контролировать запуск компонентов программного обеспечения и при обнаружении попытки запуска компонентов программного обеспечения, произведенных в нарушение установленных правил запуска компонентов программного обеспечения, выполнять [выбор: ***оповещение субъекта доступа, выполняющего запуск, и уполномоченных привилегированных субъектов; блокирование попытки запуска;*** **[назначение:** ***иные действия*****]].**

FDP_RSP_EXT.2.2

Функциональные возможности безопасности операционной системы должны контролировать целостность компонентов программного обеспечения, разрешенного для запуска, и при обнаружении попытки запуска компонентов программного обеспечения, целостность которых была нарушена, выполнять [выбор: ***оповещение субъекта доступа, выполняющего запуск, и уполномоченных привилегированных субъектов; блокирование попытки запуска*****; [назначение:** ***иные действия*****]].**

А.3. Класс FPT «Защита функциональных возможностей безопасности»

А.3.1. Монитор обращений (FPT_MTR_EXT)

Характеристика семейства

Семейство FPT_MTR_EXT «Монитор обращений» определяет компоненты требований, направленные на обеспечение операционной системой постоянного контроля обращений субъектов доступа к объектам доступа, проверки правомочности обращений в соответствии с установленными политиками и правилами управления доступом (задаются на основе компонентов из семейств FDP_ACC, FDP_ACF) и (или) управления информационными потоками (задаются на основе компонентов из семейств FDP_IFC, FDP_IFF).

Ранжирование компонентов

FPT_MTR_EXT.1 «Монитор обращений» предназначен для задания требований, связанных с обеспечением постоянного контроля обращений субъектов доступа к объектам доступа, проверки правомочности обращений в соответствии с установленными политиками и правилами управления доступом и (или) управления информационными потоками.

Управление: FPT_MTR_EXT.1

Действия по управлению не определены.

Аудит: FPT_MTR_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPT_MTR_EXT.1 Монитор обращений

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPT_MTR_EXT.1.1

Функциональные возможности безопасности операционной системы должны осуществлять постоянный контроль обращений [выбор: *субъектов доступа к объектам доступа, субъектов доступа к информации,* [назначение: *иные типы обращений*]].

FPT_MTR_EXT.1.2

Функциональные возможности безопасности операционной системы должны осуществлять проверку правомочности обращений к информации на основе установленных политик [выбор: *политика управления доступом, политика управления информационными потоками*].

FPT_MTR_EXT.1.3

Функциональные возможности безопасности операционной системы должны отклонять или удовлетворять обращения на доступ к информации по результатам проверки их правомочности.

А.3.2. FPT_APW_EXT Защита хранимой аутентификационной информации

Характеристика семейства

Семейство FPT_APW_EXT «Защита хранимой аутентификационной информации» определяет компоненты требований, направленные на защиту хранимой аутентификационной информации от раскрытия.

Ранжирование компонентов

FPT_APW_EXT.1 «Защита хранимой аутентификационной информации» предназначен для задания требований, связанных с тем, чтобы объект оценки не хранил аутентификационную информацию в открытом виде, а также, чтобы объект оценки предотвращал чтение аутентификационной информации в открытом виде.

Управление: FPT_APW_EXT.1

Действия по управлению не определены

Аудит: FPT_APW_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPT_APW_EXT.1 Защита хранимой аутентификационной информации

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPT_APW_EXT.1.1

Функциональные возможности безопасности должны предотвращать хранение аутентификационной информации в открытом виде.

FPT_APW_EXT.1.2

Функциональные возможности безопасности должны предотвращать чтение аутентификационной информации в открытом виде.

А.4. Класс FRU «Использование ресурсов»

А.4.1. Приоритет обслуживания (семейство FRU_PRS_EXT)

Характеристика семейства

Семейство FRU_PRS_EXT «Приоритет обслуживания» определяет компоненты требований, направленные на приоритизацию процессов.

Ранжирование компонентов

FRU_PRS_EXT.3 «Приоритизация процессов» предназначен для задания требований, связанных с функциональными возможностями безопасности операционной системы, обеспечивающими приоритизацию процессов, а также выделение ресурсов, доступных для разных процессов, обрабатываемых одновременно (в течение определенного периода времени).

Управление: FRU_PRS_EXT.3

Для функций управления из класса FMT может рассматриваться следующее действие:

назначение приоритетов каждому атрибуту процессов.

Аудит: FRU_PRS_EXT.3

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) Минимальный: отклонение (задержка) процесса на основании использования приоритетов атрибутов процессов при распределении ресурса операционной системы.

б) Базовый: все попытки использования функциональных возможностей распределения ресурсов операционной системы с учетом приоритетности выполнения процессов.

FRU_PRS_EXT.3 Приоритизация процессов

Иерархический для: Нет подчиненных компонентов.

Зависимости: FMT_MSA.1 Управление атрибутами безопасности
FMT_MTD.1 Управление данными функциональных возможностей безопасности

FRU_PRS_EXT.3.1

Функциональные возможности безопасности операционной системы должны осуществлять приоритизацию процессов на основе установленных приоритетов значений атрибутов процессов [назначение: *атрибуты процессов, используемые для приоритизации*] и заданной функции определения приоритета процесса на основе приоритетов значений атрибутов процесса.

FRU_PRS_EXT.3.2

Функциональные возможности безопасности операционной системы должны обеспечить выполнение процессов [назначение: *типы процессов*] и (или) доступ к вычислительным ресурсам на основе приоритизации процессов.

Приложение Б

Расширенные (специальные) компоненты требований доверия к безопасности объекта оценки

Для ОО определены следующие расширенные (специальные) компоненты требований доверия к безопасности: ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы» и AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы», 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».

Б.1. Класс ALC «Поддержка жизненного цикла»

Б.1.1. Процедуры обновления программного обеспечения операционной системы (ALC_FPU_EXT)

Цели

Процедуры обновлений программного обеспечения должны быть разработаны, реализованы и подвергнуты контролю испытательной лабораторией в целях качественного проведения работ по устранению уязвимостей операционной системы, а также недопущения внесения уязвимостей в операционную систему при ее обновлении.

ALC_FPU_EXT.1 Процедуры обновления программного обеспечения ОС

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 операционной системы для [выбор: *обновление, направленное на устранение уязвимостей ОО; иное обновление, оказывающее влияние на безопасность ОО; обновление, не оказывающее влияния на безопасность ОО*].

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

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

ALC_FPU_EXT.1.4D Заявитель (разработчик, производитель) должен разработать и реализовать процедуру предоставления

	обновлений потребителям ОС, 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 ОС должна содержать описание технологии выпуска обновлений ОС.
ALC_FPU_EXT.1.2C	Документация ОС должна содержать регламент обновления ОС, 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 ОС должен предусматривать включение в эксплуатационную документацию на выпускаемые обновления 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.

Б.1.2. Определение жизненного цикла (ALC_LCD)

ALC_LCD_EXT.3 Определенные разработчиком сроки поддержки

Зависимости: отсутствуют.

Элементы действий (разработчика, производителя)

ALC_LCD_EXT.3.1D Заявитель, разработчик, производитель должны установить в совместной декларации срок [назначение: *срок*], в течение которого они обязуются выполнять все необходимые действия по поддержке ОО, направленные на обеспечение поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2D Заявитель, разработчик, производитель должны обеспечить представление совместной декларации о сроке поддержки ОО вместе с заявкой на сертификацию ОО.

Элементы содержания и представления документированных материалов

ALC_LCD_EXT.3.1C Декларация о сроке поддержки ОО должна содержать план поддержки ОО на весь задекларированный срок, включающий описание всех предпринимаемых действий по обеспечению поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2C Декларация о сроке поддержки ОО должна содержать сведения о поддерживаемой версии ОО.

Элементы действий испытательной лаборатории

ALC_LCD_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 ALC_LCD_EXT.3.1C и ALC_LCD_EXT.3.2C.

Б.2. Класс АМА «Поддержка доверия»

Б.2.1. Анализ влияния на безопасность (AMA_SIA)

Цели

Назначение семейства AMA_SIA состоит в том, чтобы убедиться в поддержке доверия к ОО посредством анализа, проводимого разработчиком, по определению влияния на безопасность всех изменений, воздействующих на ОО после его сертификации.

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность ОС

Иерархический для: нет подчиненных компонентов.

Зависимости: ALC_FPU_EXT.1 Процедуры обновления программного обеспечения ОС.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность операционной системы должны содержать краткое описание влияния обновлений на задание по безопасности, реализацию операционной системой 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 операционную систему.

AMA_SIA_EXT.3.2C Материалы анализа влияния обновлений на безопасность ОС для обновлений, влияющих на безопасность, должны идентифицировать функции безопасности и компоненты ОС, 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 ОС.

AMA_SIA_EXT.6 Анализ влияния внешних модулей уровня ядра на безопасность операционной системы

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

AMA_SIA_EXT.6.1D Разработчик (заявитель, производитель) должен предоставлять в испытательную лабораторию материалы анализа влияния внешних модулей уровня ядра на безопасность операционной системы и комплект идентифицированных (промаркированных) внешних модулей уровня ядра.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.6.1C Материалы анализа влияния внешних модулей уровня ядра на безопасность операционной системы должны содержать краткое описание влияния внешних модулей уровня ядра на задание по безопасности, функции безопасности операционной системы или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.6.2C Материалы анализа влияния внешних модулей уровня ядра операционной системы на безопасность операционной системы, должны идентифицировать функции безопасности и компоненты операционной системы, на которые влияют внешние модули уровня ядра.

Элементы действий испытательной лаборатории

AMA_SIA_EXT.6.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению документированных материалов.

AMA_SIA_EXT.6.2E Испытательная лаборатория должна подтвердить влияние (отсутствие влияния) внешних модулей уровня ядра на безопасность операционной системы.