ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Экз. №

Утвержден ФСТЭК России
11 мая 2017 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ ТИПА «В» ПЯТОГО КЛАССА ЗАЩИТЫ

ИТ.ОС.В5.ПЗ

МОСКВА
2017

В книге всего пронумеровано 106 страниц, несекретно

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» пятого класса защиты.
Тип ОС:	ОС типа «В».
Класс защиты:	Пятый.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.ОС.В5.ПЗ.
Идентификация ОО:	ОС типа «В» пятого класса защиты.
Уровень доверия:	Оценочный уровень доверия 2 (ОУД2), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS. 5 «Полный полуформальный модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов».
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») пятого 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.

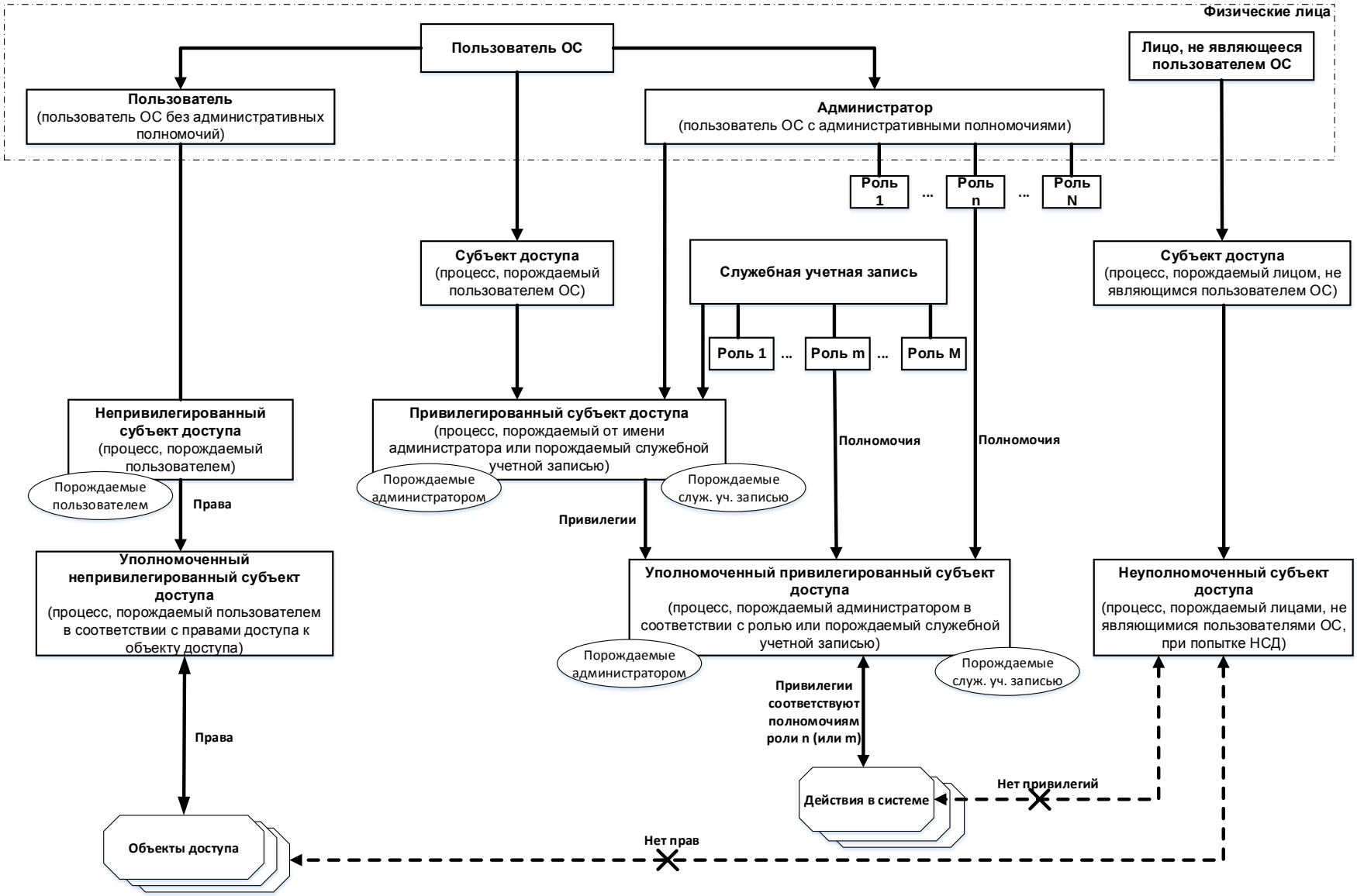

Рисунок 2.1 – Соотношение терминов, применяемых в профиле защиты для обозначения пользователей ОС и субъектов доступа разных категорий

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»:

идентификацию и аутентификацию 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;

обеспечение недоступности остаточной информации при распределении или освобождении ресурса памяти для непривилегированных субъектов доступа;

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;

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

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

возможность обеспечения надежных меток времени при проведении аудита безопасности;

возможность тестирования (самотестирования) функций безопасности ОС, проверки целостности ПО ОС и целостности данных (параметров) ОС;

возможность обеспечения восстановления штатного режима функционирования ОС;

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;

поддержку 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 выполнения действий, направленные на предотвращение потери данных аудита при переполнении журнала аудита;

возможность полнотекстовой регистрации привилегированных команд (команд, управляющих системными функциями);

возможность регистрации возникновения событий, которые в соответствии с ГОСТ Р ИСО/МЭК 15408-2 включены в базовый 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 2 (ОУД2), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS. 5 «Полный полуформальный модульный проект», ALC_FLR.1 «Базовое устранение недостатков»,

AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов».

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» – операционная система, 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 **«назначение»** 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» (ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», 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», AVA_CCA_EXT.1 «Анализ скрытых каналов», 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», 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 2 (ОУД2), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS. 5 «Полный полуформальный модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки»,

ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов».

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. Определение проблемы безопасности

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

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

политик безопасности, которые должен выполнять ОО;

предположений безопасности (обязательных условий безопасного использования ОО).

4.1. Угрозы

4.1.1. Угрозы, которым должен противостоять объект оценки

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

Угроза-1

1. Аннотация угрозы – несанкционированный доступ к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – осуществление несанкционированного доступа субъектов доступа к объектам файловой системы и устройствам, нарушение правил управления доступом к объектам файловой системы и устройствам, программное воздействие на интерфейс программирования приложений, переполнение буфера.

4. Используемые уязвимости – недостатки механизмов управления доступом, связанные с возможностью осуществления несанкционированного доступа к объектам файловой системы и устройствам.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, содержащаяся в объектах файловой системы, устройства.

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

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, размещаемой на СВТ, несанкционированные действия по отношению к объектам файловой системы и устройствам.

Угроза-2

1. Аннотация угрозы – 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 ресурсов на их обработку.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – выполнение запросов и иные обращения к ОС, связанные с расходованием ресурсов СВТ (времени процессора, оперативной и внешней памяти): загрузка процессора бесконечными вычислениями, нецелевое расходование памяти за счет деструктивного использования механизма рекурсии и др.

4. Используемые уязвимости – недостатки механизмов балансировки нагрузки и распределения (ограничения использования) вычислительных ресурсов СВТ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, обрабатываемая на СВТ.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Возможные последствия реализации угрозы – недоступность информации, обрабатываемой на СВТ, для пользователей ОС.

Угроза-3

1. Аннотация угрозы – несанкционированное или ошибочное удаление информации со средства вычислительной техники, функционирующего под управлением ОС.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – осуществление несанкционированного или ошибочного удаления информации при наличии прав на удаление информации.

4. Используемые уязвимости – недостатки механизмов обеспечения резервирования и восстановления защищаемой информации на СВТ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, содержащаяся в объектах файловой системы.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Возможные последствия реализации угрозы – отсутствие на СВТ информации, требуемой для пользователей ОС.

Угроза-4

1. Аннотация угрозы – утечка или несанкционированное изменение информации в оперативной памяти, используемой различными процессами и формируемыми ими потоками данных.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – осуществление доступа к сегментам (областям, блокам) оперативной памяти, используемой процессами и формируемыми ими потоками данных, или к сегментам (областям, блокам) оперативной памяти, в которых расположен буфер обмена для кэширования данных.

4. Используемые уязвимости – недостатки механизмов обеспечения недоступности процессов обработки информации в ОС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация в оперативной памяти СВТ.

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

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и (или) нарушение целостности информации, запрашиваемой процессами обработки информации, несанкционированная модификация потоков данных, формируемых процессами обработки информации для внесения изменений в объекты файловой системы и обращения к устройствам СВТ.

Угроза-5

1. Аннотация угрозы – несанкционированное внесение нарушителем изменений в конфигурационные (и иные) данные, которые влияют на функционирование отдельных сервисов, приложений или ОС в целом.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – внесение изменений в системный реестр или иной каталог конфигурационных данных.

4. Используемые уязвимости – недостатки механизмов контроля доступа к системному реестру (или иному каталогу конфигурационных данных).

5. Вид информационных ресурсов, потенциально подверженных угрозе – конфигурационные данные ОС.

6. Нарушаемое свойство безопасности активов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение штатных режимов функционирования системного и прикладного программного обеспечения.

Угроза-6

1. Аннотация угрозы – осуществление восстановления (подбора) аутентификационной информации пользователей ОС.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – подбор аутентификационной информации.

4. Используемые уязвимости – недостатки механизмов идентификации и аутентификации; возможность доступа к месту хранения аутентификационной информации.

5. Вид информационных ресурсов, потенциально подверженных угрозе –информация, обрабатываемая на СВТ; данные аудита.

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

7. Возможные последствия реализации угрозы – осуществление несанкционированных действий по отношению к объектам файловой системы и устройствам с использованием полномочий скомпрометированной учетной записи пользователя ОС; недостоверность данных аудита (все действия, выполненные нарушителем, будут ассоциированы с пользователем ОС, который этих действий не совершал).

Угроза-7

1. Аннотация угрозы – использование нарушителем идентификационной и начальной аутентификационной информации, соответствующей учетной записи пользователя ОС.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – преодоление механизмов идентификации и (или) аутентификации ОС за счет использования полученной нарушителем идентификационной и начальной аутентификационной информации пользователя ОС.

4. Используемые уязвимости – недостатки механизмов идентификации и аутентификации в ОС в части задания характеристик начальной аутентификационной информации, в части механизма контроля смены начальной аутентификационной информации.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, обрабатываемая на СВТ; устройства; данные аудита.

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

7. Возможные последствия реализации угрозы – осуществление несанкционированных действий по отношению к объектам доступа с использованием полномочий скомпрометированной учетной записи пользователя ОС, в объеме его полномочий; недостоверность данных аудита (все действия, выполненные нарушителем, будут ассоциированы с пользователем ОС, который этих действий не совершал).

Угроза-8

1. Аннотация угрозы – несанкционированное внесение изменений в журналы регистрации событий безопасности ОС.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – осуществление несанкционированного доступа к журналам регистрации событий безопасности ОС с возможностью его редактирования.

4. Используемые уязвимости – недостатки механизмов управления доступом к журналам регистрации событий безопасности ОС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, размещаемая в журналах регистрации событий безопасности ОС.

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

7. Возможные последствия реализации угрозы – нарушение подотчетности пользователей ОС за свои действия; необнаружение администратором фактов нарушения безопасности информации; недостоверность данных аудита.

Угроза-9

1. Аннотация угрозы – несанкционированный доступ к информации вследствие использования пользователями ОС неразрешенного программного обеспечения.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – установка в ОС компонентов неразрешенного программного обеспечения.

4. Используемые уязвимости – недостатки механизмов контроля установки программного обеспечения.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, обрабатываемая на СВТ.

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

7. Возможные последствия реализации угрозы – несанкционированный доступ к объектам файловой системы и устройствам, недоступность объектов файловой системы и устройств для пользователей ОС, несанкционированные действия по отношению к объектам файловой системы и устройствам.

Угроза-10

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

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – доступ к объектам доступа, созданным другим пользователем ОС; доступ к остаточной информации, оставшейся после сеанса работы другого пользователя ОС.

4. Используемые уязвимости – недостатки механизмов управления доступом; недостатки механизмов очистки остаточной информации.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, размещаемая в объектах ОС.

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

7. Возможные последствия реализации угрозы – несанкционированные действия по отношению к объектам файловой системы и устройствам.

Угроза- 11

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

2. Источники угрозы – программное обеспечение ОС, внутренний нарушитель.

3. Способ реализации угрозы – запуск критичных служб и приложений совместно с менее критичными службами и приложениями в условиях отсутствия управления приоритетами их выполнения.

4. Используемые уязвимости – недостатки механизмов распределения ресурсов между потоками служб и приложений и (или) их настройки.

5. Вид информационных ресурсов, потенциально подверженных угрозе – потоки критичных служб и приложений, вычислительные ресурсы.

6. Нарушаемые свойства безопасности информационных ресурсов – доступность.

7. Возможные последствия реализации угрозы – недоступность вычислительных ресурсов (процессорное время, оперативная память) для критичных служб ОС и функционирующего прикладного программного обеспечения.

4.1.2. Угрозы, которым противостоит среда

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

Угроза среды-1

1. Аннотация угрозы – нарушение целостности программных компонентов ОС.

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

3. Способ реализации угрозы – действия, направленные на несанкционированные изменения программных компонентов ОС.

4. Используемые уязвимости – недостатки механизмов защиты компонентов ОС.

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

6. Нарушаемые свойства безопасности информационных ресурсов – целостность.

7. Возможные последствия реализации угрозы – нарушение целостности компонентов ОС, нарушение режимов функционирования ОС.

Угроза среды-2

1. Аннотация угрозы отключение и (или) обход нарушителями компонентов ОС, реализующих функции безопасности информации путем подмены нарушителем загружаемой ОС.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированное изменение пути доступа к загрузчику ОС (в конфигурации базовой системы ввода-вывода, если применимо).

4. Используемые уязвимости – недостатки управления доступом к загрузке ОС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, обрабатываемая на СВТ.

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

7. Возможные последствия реализации угрозы – несанкционированный доступ к информации, обрабатываемой на СВТ, нарушение режимов функционирования ОС и СВТ.

Угроза среды-3

1. Аннотация угрозы – нарушение целостности данных (в том числе параметров настройки средств защиты информации) ОС.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – доступ к контейнерам (файлам), в которых хранятся конфигурационные данные функций безопасности ОС до ее загрузки.

4. Используемые уязвимости – недостатки контроля физического доступа к СВТ, на которых функционирует ОС.

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

6. Нарушаемые свойства безопасности информационных ресурсов – целостность.

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

Угроза среды-4

1. Аннотация угрозы – несанкционированный доступ нарушителя к аутентификационной информации администраторов и (или) пользователей ОС.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – доступ к контейнерам (файлам), в которых хранится аутентификационная информация (или ее образы) пользователей ОС до загрузки ОС.

4. Используемые уязвимости – недостатки контроля физического доступа к СВТ, на которых функционирует ОС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – аутентификационная информация (пароли) пользователей ОС.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированный доступ в ОС.

Угроза среды-5

1. Аннотация угрозы – несанкционированное внесение нарушителем изменений в журналы регистрации событий безопасности ОС за счет доступа к файлам журналов регистрации событий безопасности ОС в среде функционирования ОС с использованием специальных программных средств, предоставляющих возможность обрабатывать файлы журналов регистрации событий безопасности ОС.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – осуществление несанкционированного доступа к журналам регистрации событий безопасности ОС за счет доступа к файлам журналов регистрации событий безопасности ОС до загрузки ОС.

4. Используемые уязвимости – недостатки контроля физического доступа к СВТ, на которых функционирует ОС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, содержащаяся в журналах регистрации событий безопасности ОС.

6. Нарушаемые свойства безопасности информационных ресурсов – целостность.

7. Возможные последствия реализации угрозы – нарушение подотчетности пользователей ОС за свои действия; необнаружение администратором фактов нарушения безопасности информации.

Угроза среды-6

1. Аннотация угрозы – несанкционированное копирование информации из памяти средств вычислительной техники на съемные машинные носители информации (или в другое место вне информационной системы) пользователем ОС.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – копирование объектов файловой системы с использованием предоставленных субъекту доступа прав в момент обработки защищаемой информации на съемный машинный носитель для отчуждения из информационной системы и дальнейшего неправомерного использования.

4. Используемые уязвимости – недостатки контроля за действиями пользователей ОС; недостатки организационных мер защиты информации в ИС, дающие возможность нарушителям неконтролируемого вноса в контролируемую зону неразрешенных съемных машинных носителей информации и выноса любых съемных машинных носителей информации; недостатки механизмов аудита событий копирования информации на съемные машинные носители информации.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, обрабатываемая на СВТ.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность.

7. Возможные последствия реализации угрозы – неправомерное использование защищаемой информации, в том числе ознакомление с ней неограниченного круга неуполномоченных лиц.

Угроза среды-7

1. Аннотация угрозы – снижение производительности ОС из-за внедрения в нее избыточного программного обеспечения и его компонентов.

2. Источники угрозы – внутренний нарушитель.

3. Способ реализации угрозы – внедрение в ОС избыточного программного обеспечения и системных компонентов.

4. Используемые уязвимости – недостатки контроля установки программного обеспечения.

5. Вид информационных ресурсов, потенциально подверженных угрозе – программное обеспечение, информационная система, ключевая система информационной инфраструктуры.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение штатных режимов функционирования системного и прикладного программного обеспечения ОС в ИС.

4.2. Политика безопасности

ОО должен выполнять приведенные ниже политики безопасности.

Политика безопасности-1

Должны осуществляться идентификация и аутентификация пользователей ОС до выполнения любых действий по доступу в информационную систему или по управлению ОС.

Политика безопасности-2

В ОО для управления доступом субъектов доступа (пользователей ОС и процессов, запускаемых от имени пользователей ОС) к объектам доступа в ОС (объектам файловой системы, записям реестра и (или) иным объектам доступа) должно быть реализовано дискреционное и(или) ролевое управление доступом.

Замечание по применению: При изложении данной политики безопасности в задании по безопасности допускаются следующие сочетания реализации методов управления доступом:

дискреционное и ролевое управление доступом;

дискреционное управление доступом;

ролевое управление доступом.

Если ОО реализует мандатное управление доступом, в ЗБ следует включить соответствующие компоненты ФТБ, уточнить соответствующую цель безопасности.

Политика безопасности-3

Должна осуществляться возможность задания правил управления доступом, разрешающих или запрещающих доступ субъектов доступа к объектам доступа (объектам файловой системы, записям реестра и (или) иным объектам доступа), а также определяющих разрешенные типы доступа (операции: создание объекта файловой системы, модификация объекта файловой системы, удаление объекта файловой системы, добавление данных в объект файловой системы, удаление данных из объекта файловой системы; модификация данных в объекте файловой системы, чтение информации из объекта файловой системы, запуск исполняемых объектов файловой системы, установка компонентов программного обеспечения) с использованием атрибутов безопасности объектов доступа и субъектов доступа на основе реализованных в ОС методов управления доступом (дискреционный, ролевой).

Политика безопасности-4

Должны обеспечиваться возможности генерирования надежных меток времени.

Политика безопасности-5

Должна обеспечиваться возможность очистки остаточной информации в памяти средства вычислительной техники при ее освобождении (распределении) или блокирование доступа субъектов доступа к остаточной информации.

Политика безопасности-6

Должна обеспечиваться изоляция программных модулей одного процесса (одного субъекта доступа) от программных модулей других процессов (других субъектов доступа).

Политика безопасности-7

Должны обеспечиваться восстановление функциональных возможностей безопасности и настроек (параметров) ОС после сбоев и отказов; сохранение штатного режима функционирования и (или) корректное восстановление штатного режима функционирования ОС при сбоях и ошибках.

Политика безопасности-8

Должны осуществляться контроль целостности компонентов операционной системы, а также иных объектов файловой системы, содержащих данные (параметры) ОС; проверка правильности выполнения функций безопасности ОС.

Политика безопасности-9

Должно осуществляться безопасное выделение областей оперативной памяти.

Политика безопасности-10

Должны обеспечиваться возможности по управлению работой ОС и параметрами ОС со стороны администраторов.

Политика безопасности-11

Должна быть обеспечена регистрация возможных событий безопасности. Механизмы регистрации должны предоставлять администратору возможность ознакомления с информацией о произошедших событиях.

Политика безопасности-12

Должны обеспечиваться контроль установки и контроль запуска компонентов программного обеспечения.

Политика безопасности-13

Должна осуществляться приоритизация процессов и выделение ресурсов, доступных для разных процессов, обрабатываемых одновременно.

Политика безопасности-14

Должны обеспечиваться контроль и проверка правомочности обращений субъектов доступа к объектам доступа.

4.3. Предположения безопасности

Предположение, связанное с физическими аспектами среды функционирования

Предположение-1

Должна быть обеспечена невозможность осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует ОС.

Предположения по отношению к аспектам связности среды функционирования

Предположение-2

Должны быть обеспечены условия технической совместимости ОС с СВТ (возможности функционирования в соответствии с установленными ФТБ) для реализации своих функциональных возможностей.

Предположение-3

Должна быть обеспечена невозможность несанкционированного внесения изменений в логику функционирования ОС через механизм обновления программного обеспечения ОС.

Предположение-4

ОС должна функционировать в соответствии с эксплуатационной документацией.

Предположение-5

Должен быть обеспечен контроль целостности внешних модулей уровня ядра, получаемых от заявителя (разработчика, производителя).

Предположение-6

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

Предположение-7

Должна обеспечиваться доверенная загрузка ОС, а также средства вычислительной техники, на котором она функционирует.

Предположение-8

Должно быть обеспечено ограничение на установку программного обеспечения и его компонентов из недоверенных источников или не задействованных в технологическом процессе обработки информации источников.

Предположение, связанное с персоналом среды функционирования

Предположение-9

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

5. Цели безопасности

5.1. Цели безопасности для объекта оценки

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Идентификация и аутентификация пользователей ОС и объектов доступа

ОО должен обеспечивать возможность идентификации и аутентификации пользователей ОС до предоставления доступа в ОС.

Цель безопасности-2

Управление доступом

ОО должен обеспечивать:

дискреционное и(или) ролевое управление доступом субъектов доступа (пользователей ОС и процессов, запускаемых от имени пользователей ОС) к объектам доступа в ОС (объектам файловой системы, записям реестра и (или) иным объектам доступа) для недопущения несанкционированного доступа к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен;

возможность задания правил управления доступом, разрешающих или запрещающих доступ субъектов доступа к объектам доступа, а также определяющих разрешенные типы доступа с использованием атрибутов безопасности объектов доступа и субъектов доступа на основе реализованных в ОС методов управления доступом (дискреционный, ролевой);

контроль и проверку правомочности обращений субъектов доступа к объектам доступа для исключения возможности несанкционированного внесения изменений в журналы регистрации событий безопасности ОС.

Замечание по применению: При изложении данной цели безопасности в задании по безопасности допускаются следующие сочетания реализации методов управления доступом:

дискреционное и ролевое управление доступом;

дискреционное управление доступом;

ролевое управление доступом.

Если ОО реализует мандатное управление доступом, в ЗБ следует включить соответствующие компоненты ФТБ, уточнить соответствующую политику безопасности.

Цель безопасности-3

Защита от несанкционированного доступа в обход правил управления доступом

ОО должен обеспечивать:

возможность обеспечения недоступности остаточной информации при распределении или освобождении ресурса памяти для исключения возможности несанкционированного доступа субъектов доступа к информации, обработка которой осуществлялась в рамках сеансов (сессий) других субъектов доступа;

изоляцию программных модулей одного процесса (одного субъекта доступа) от программных модулей других процессов (других субъектов доступа) для исключения возможности утечки или несанкционированного изменения информации в оперативной памяти, используемой различными процессами и формируемыми ими потоками данных;

контроль установки и контроль запуска компонентов программного обеспечения для исключения возможности несанкционированного доступа к информации вследствие использования пользователями ОС неразрешенного программного обеспечения;

защиту хранимой аутентификационной информации.

Цель безопасности-4

Обеспечение целостности и восстановление компонентов ОС

ОО должен обеспечивать:

контроль целостности компонентов операционной системы, а также иных объектов файловой системы, содержащих данные (параметры) ОС, проверку правильности выполнения собственных функций безопасности для исключения возможности несанкционированного внесения нарушителем изменений в конфигурационные данные, которые влияют на функционирование отдельных сервисов, приложений или ОС в целом;

возможность восстановления функциональных возможностей безопасности и настроек (параметров) ОС после сбоев и отказов, а также сохранения штатного режима функционирования и (или) корректного восстановления штатного режима функционирования ОС при сбоях и ошибках.

Цель безопасности-5

Обеспечение доступности ресурсов

ОО должен обеспечивать доступность сервисов и информации, возможность выделения вычислительных ресурсов для процессов в соответствии с их приоритетами:

для исключения возможности ограничения 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 ресурсов на их обработку;

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

Цель безопасности-6

Регистрация событий безопасности ОС

ОО должен обеспечивать:

регистрацию возможных нарушений безопасности и предупреждение (сигнализацию) о таких событиях безопасности в ОС;

возможность выборочного ознакомления администратора с информацией о произошедших событиях, а также обеспечивать подотчетность пользователей ОС за свои действия.

Цель безопасности-7

Генерирование временных меток

ОО должен обеспечивать генерирование надежных меток времени.

Цель безопасности-8

Управление ОС

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

5.2. Цели безопасности для среды функционирования

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

Цель для среды функционирования ОО-1

Совместимость

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 содержалась в тайне и была недоступна 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 умеренным потенциалом нападения.

5.3. Обоснование целей безопасности

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

Таблица 5.1 – Отображение целей безопасности для ОО на угрозы и политику безопасности.

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8
Угроза - 1	X	X						
Угроза – 2					X			
Угроза – 3				X				
Угроза – 4			X	X				
Угроза - 5		X						
Угроза – 6	X							
Угроза – 7	X							
Угроза – 8		X				X		
Угроза – 9			X					
Угроза – 10			X					
Угроза – 11					X			
Политика безопасности-1	X							
Политика безопасности-2		X						
Политика безопасности-3		X						
Политика безопасности-4							X	
Политика безопасности-5			X					
Политика безопасности-6			X					
Политика безопасности-7				X				
Политика безопасности-8				X				
Политика безопасности-9			X					
Политика безопасности-10								X
Политика безопасности-11						X		
Политика безопасности-12								
Политика безопасности-13					X			
Политика безопасности-14		X						

Цель безопасности-1

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-6, Угроза-7** и реализацией политики безопасности **Политика безопасности-1**, так как обеспечивает использование механизмов идентификации и аутентификации пользователей ОС.

Цель безопасности-2

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-5**, **Угроза-8** и реализации политик безопасности **Политика безопасности-2, Политика безопасности-3, Политика безопасности-14**, так как обеспечивает: дискреционное и(или) ролевое управление доступом; возможность задания правил управления доступом, разрешающих или запрещающих доступ субъектов доступа к объектам доступа; контроль и проверку правомочности обращений субъектов доступа к объектам доступа.

Цель безопасности-3

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-4, Угроза-9, Угроза-10** и реализации политик безопасности **Политика безопасности-5, Политика безопасности-6, Политика безопасности-9,** так как обеспечивает: возможность обеспечения недоступности остаточной информации при распределении или освобождении ресурса памяти для исключения возможности несанкционированного доступа субъектов доступа к информации, обработка которой осуществлялась в рамках сеансов (сессий) других субъектов доступа; изоляцию программных модулей одного процесса (одного субъекта доступа) от программных модулей других процессов (других субъектов доступа); контроль установки и контроль запуска компонентов программного обеспечения; защиту от выполнения произвольного машинного кода.

Цель безопасности-4

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-3, Угроза-4** и реализации политик безопасности **Политика безопасности-7, Политика безопасности-8**, так как обеспечивает: возможность восстановления функциональных возможностей безопасности и настроек (параметров) ОС после сбоев и отказов, а также сохранение штатного режима функционирования и (или) корректное восстановление штатного режима функционирования ОС при сбоях и ошибках; контроль целостности компонентов ОС и иных объектов файловой системы, а также возможность осуществления проверки правильности выполнения собственных функций безопасности.

Цель безопасности-5

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-2**, **Угроза-11** и реализации политики безопасности **Политика безопасности-13**, так как обеспечивает выделение вычислительных ресурсов в соответствии с приоритетами.

Цель безопасности-6

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-8** и реализации политики безопасности **Политика безопасности-11,** так как обеспечивает возможность регистрации событий, относящихся к возможным нарушениям безопасности, и ознакомления администратора с информацией о произошедших событиях.

Цель безопасности-7

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-4**, так как обеспечивает возможность генерирования меток времени и (или) синхронизации системного времени.

Цель безопасности-8

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-10**, так как обеспечивает возможность управления работой ОС и параметрами ОС со стороны администраторов.

6. Определение расширенных компонентов

В данном разделе ПЗ представлены расширенные компоненты для ОС.

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

Для ОО определены 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.

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

Для ОО определены следующие расширенные (специальные) компоненты требований доверия к безопасности: ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов», 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.

7. Требования безопасности

В данном разделе ПЗ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности». Кроме того, в настоящий ПЗ включено ряд требований безопасности, сформулированных в явном виде (расширение национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности»). Требования доверия основаны на компонентах требований доверия из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД2, усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS. 5 «Полный полуформальный модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов», 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»).

7.1. Функциональные требования безопасности объекта оценки

Функциональные компоненты из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности», на которых основаны функциональные требования безопасности ОО, а также компоненты сформулированных в явном виде расширенных (специальных) требований приведены в таблице 7.1.

Таблица 7.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	**Название компонента требований**
FAU_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
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_RIP.1	Ограниченная защита остаточной информации
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

Окончание таблицы 7.1

Идентификатор компонента требований	Название компонента требований
FPT_APW_EXT.1	Защита хранимой аутентификационной информации
FPT_TST.1	Тестирование функциональных возможностей безопасности
FPT_RCV.2	Автоматическое 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

7.1.1. 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 *базовом* уровне аудита;

в) [события, приведенные во втором столбце таблицы 7.2, 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 7.2 – 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
FMT_MOF.1 FMT_MSA.1 FMT_MTD.1	Полнотекстовая запись привилегированных команд (команд, управляющих системными функциями)	
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.

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны [выбор (выбрать одно из): *предотвращать события, подвергающиеся аудиту, исключая предпринимаемые уполномоченным привилегированным субъектом доступа; записывать поверх самых старых хранимых записей аудита; **записывать действия уполномоченных привилегированных субъектов доступа поверх старых хранимых записей аудита***] и [назначение: *другие действия, которые нужно предпринять в случае возможного сбоя хранения журнала **регистрации событий безопасности ОС***] при переполнении журнала **регистрации событий безопасности ОС.**

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита.

7.1.2. 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_RIP.1 Ограниченная защита остаточной информации

FDP_RIP.1.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при [выбор: *распределение ресурса, освобождение ресурса*] для следующих объектов: [назначение: *список объектов*].

Зависимости: отсутствуют.

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.

7.1.3. 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.

7.1.4. Управление безопасностью (FMT)

FMT_SMF.1 Спецификация функций управления

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

Зависимости: отсутствуют.

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.

7.1.5. Защита ФБО (FPT)

FPT_TST.1 **Тестирование функциональных возможностей безопасности**

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

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

FPT_TST.1.3 ФБО должны предоставить **администратору** возможность верифицировать целостность хранимого выполняемого кода ФБО.

Зависимости: отсутствуют.

Замечания по применению: компонент предназначен для задания требований к функциональным возможностям ОО по осуществлению контроля целостности компонентов операционной системы, а также иных объектов файловой системы, содержащих данные (параметры) операционной системы, проверки правильности выполнения собственных функций безопасности ОС.

FPT_STM.1 **Надежные метки времени**

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

Зависимости: отсутствуют.

FPT_RCV.2 **Автоматическое восстановление**

FPT_RCV.2.1 Когда автоматическое восстановление после [назначение: *список сбоев/ прерываний обслуживания*] невозможно, ФБО

должны перейти в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

FPT_RCV.2.2 Для [назначение: *список сбоев/прерываний обслуживания*] ФБО должны обеспечить возврат ОО к безопасному состоянию с использованием автоматических процедур.

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.

7.1.6. 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:

1. 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.
2. 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.
3. 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.
4. 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.

7.1.7. 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.

7.2. Требования доверия к безопасности объекта оценки

Требования доверия к безопасности ОО взяты из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» и образуют ОУД2, усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках», ADV_TDS. 5 «Полный полуформальный модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов» (см. таблицу 7.3).

Таблица 7.3 – Требования доверия к безопасности ОО

Класс доверия	**Идентификатор компонента доверия**	**Название компонента доверия**
Разработка	ADV_ARC.1	Описание архитектуры безопасности
	ADV_FSP.5	Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках
	ADV_IMP.2*	Полное отображение представления реализации ФБО
	ADV_IMP_EXT.3	Реализация ОО
	ADV_TDS.5	Полный полуформальный модульный проект
Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_PRE.1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC.2	Использование системы УК
	ALC_CMS.2	Охват УК частей ОО
	ALC_DEL.1	Процедуры поставки
	ALC_FLR.1	Базовое устранение недостатков
	ALC_TAT_EXT.0	Определение инструментальные средства разработки
	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.2	Цели безопасности
	ASE_REQ.2	Производные требования безопасности
	ASE_SPD.1	Определение проблемы безопасности
	ASE_TSS.1	Краткая спецификация ОО

Окончание таблицы 7.3

Класс доверия	Идентификатор компонента доверия	Название компонента доверия
Тестирование	ATE_COV.1	Свидетельство покрытия
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_VAN.4	Методический анализ уязвимостей
	AVA_CCA_EXT.1	Анализ скрытых каналов
Поддержка доверия	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
* – Отмечены компоненты, конкретизированные в настоящем ПЗ для обеспечения преемственности требованиям по контролю отсутствия недекларированных возможностей, изложенных в руководящем документе «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации: Классификация по уровню контроля отсутствия недекларированных возможностей», (Гостехкомиссия России, 1999).		

7.2.1. Разработка (ADV)

ADV_ARC.1 Описание архитектуры безопасности

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

Элементы действий заявителя (разработчика, производителя)

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

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

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

Элементы содержания и представления документированных материалов

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

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

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

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

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

Элементы действий испытательной лаборатории

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

Замечания по применению:

1. Архитектура безопасности должна обеспечивать, чтобы ОО не имел каналов связи, обеспечивающих доступ (в том числе внеполосный) в обход заданных правил управления доступом к ОО (ее программному обеспечению и настройкам), а также правил контроля и фильтрации сетевого трафика (сетевых потоков).
2. Испытательная лаборатория должна выполнять указанные действия в соответствии с пунктом 10.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ADV_FSP.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_IMP.2 Полное отображение представления реализации ФБО

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

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления документированных материалов

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

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

ADV_IMP.2.3C В прослеживании между всем представлением реализации и описанием проекта ОО **(для всех модулей, отнесенных к осуществляющим или поддерживающим выполнение ФТБ)** должно быть продемонстрировано их соответствие, **а для модулей изделия, определенных как «не влияющие на выполнение ФТБ», должно быть предоставлено соответствующее обоснование**.

Элементы действий испытательной лаборатории

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

а) контроля исходного состояния ПО;

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

Замечания по применению:

1. В ADV_IMP.2.1E контроль исходного состояния ПО предусматривает фиксацию состава ПО и документации на него и сравнение с описанием, представленным в документации. При фиксации также должен быть выполнен расчет уникальных значений контрольных сумм файлов с исходными текстами программ, входящих в состав ПО. Контрольные суммы должны рассчитываться для каждого файла.

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

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

4. Испытательная лаборатория при контроле отсутствия избыточности исходных текстов должна:

в части модулей, осуществляющих и поддерживающих выполнение ФТБ, – исследовать (основываясь на структурном анализе и декомпозиции) эти модули, чтобы сделать заключение об отсутствии в исходных текстах функциональных возможностей безопасности, не предусмотренных проектом и ФТБ;

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

ADV_IMP_EXT.3 Реализация ОО

Зависимости: ADV_IMP.2 Полное отображение представления реализации ФБО.

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления документированных материалов

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

ADV_IMP_EXT.3.2C В прослеживании между реализацией ОО и представлением реализации должно быть продемонстрировано *соответствие между реализацией ПО: загрузочные модули ПО,* [назначение*: иные типы элементов реализации ПО*] *и их представлением реализации: исходные тексты ПО,* [назначение*: иные формы представления реализации*].

Элементы действий испытательной лаборатории

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

Замечания по применению: при осуществлении операций «выбор» и «назначение» в элементах ADV_IMP_EXT.3.1C и ADV_IMP_EXT.3.2C в качестве типов элементов реализации программного обеспечения ОС могут рассматриваться:

загрузчик операционной системы;
ядро операционной системы;
модули уровня ядра;
модули служб ОС;
иные компоненты программного обеспечения ОС.

ADV_TDS.5 Полный полуформальный модульный проект

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

Элементы действий заявителя (разработчика, производителя)

ADV_TDS.5.1D Разработчик должен представить проект ОО.

ADV_TDS.5.2D Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Элементы содержания и представления документированных материалов

ADV_TDS.5.1C В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV_TDS.5.2C В проекте должно приводиться описание структуры ОО на уровне модулей, с присвоением каждому модулю категории либо осуществляющего выполнение ФТБ, либо поддерживающего, либо не влияющего на выполнение ФТБ.

ADV_TDS.5.3C В проекте должны быть идентифицированы все подсистемы ФБО.

ADV_TDS.5.4C В проекте должно приводиться полуформальное описание каждой из подсистем ФБО, сопровождающееся вспомогательным пояснительным неформальным текстом, если это представляется уместным.

ADV_TDS.5.5C В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV_TDS.5.6C В проекте должно быть осуществлено прослеживание подсистем ФБО к модулям ФБО.

ADV_TDS.5.7C В проекте должно приводиться полуформальное описание каждого модуля с точки зрения его назначения, взаимодействия с другими модулями, интерфейсов и значений, предоставляемых этими интерфейсами в ответ на запросы, а также вызываемых интерфейсов других модулей. Полуформальное описание сопровождается вспомогательным пояснительным неформальным текстом, если это представляется целесообразным.

ADV_TDS.5.8C В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий испытательной лаборатории

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

ADV_TDS.5.2E Испытательная лаборатория должна сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

7.2.2. Руководства (AGD)

AGD_OPE.1 Руководство пользователя по эксплуатации

Зависимости: ADV_FSP.1 Базовая функциональная спецификация.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

AGD_OPE.1.1C В руководстве пользователя **ОС** по эксплуатации для каждой роли **пользователя ОС** должно быть представлено описание доступных пользователям **ОС** функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.

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

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

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

AGD_OPE.1.5C В руководстве пользователя **ОС** 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 **ОС** по эксплуатации для каждой роли **пользователя ОС** должно быть **приведено** описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ**, имеющих отношение к пользователю ОС**.

AGD_OPE.1.7C Руководство пользователя **ОС** 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:

1. Материал по администрированию ОС, соответствующий ролям администраторов, включается в «Руководство администратора». Материал, соответствующий роли пользователя, включается в «Руководство пользователя».

2. 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:

1. Материал подготовительных процедур включается в «Руководство администратора», детализация подготовительных процедур в части безопасной настройки ОС – в «Правила по безопасной настройке».
2. 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».
3. Документированные материалы должны содержать свидетельства отсутствия в ОО 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.
4. Документированные материалы должны содержать свидетельства отсутствия в ОО 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.

5. Документированные материалы должны содержать свидетельства, включающие описания всех возможностей по управлению для каждой ФБО, в том числе используемых управляемых сущностей (механизмы, интерфейсы, правила, каналы и т.д.), способов администрирования ОО (локальное, удаленное), ролей администраторов в соответствии с FMT_SMR.1, которым предоставлены возможности по управлению, а для неиспользуемых возможностей по управлению ФБО должно быть представлено соответствующее обоснование.

7.2.3. Поддержка жизненного цикла (ALC)

ALC_CMC.2 Использование системы УК

Зависимости: ALC_CMS.1 Охват УК ОО.

Элементы действий заявителя (разработчика, производителя)

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

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

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

Элементы содержания и представления документированных материалов

ALC_CMC.2.1C ОО должен быть помечен уникальной маркировкой.

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

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

Элементы действий испытательной лаборатории

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

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

ALC_CMS.2 Охват УК частей ОО

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

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

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

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

Элементы действий испытательной лаборатории

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

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

ALC_DEL.1 Процедуры поставки

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления документированных материалов

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

Элементы действий испытательной лаборатории

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

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

ALC_FLR.1 Базовое устранение недостатков

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

ALC_FLR.1.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

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

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

ALC_FLR.1.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям **ОС** информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Элементы действий испытательной лаборатории

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

Замечания по применению:

1. Для выполнения данных требований заявитель (разработчик, производитель) должен осуществлять постоянный поиск и устранение уязвимостей и других недостатков в ОС и выпуск соответствующих обновлений программной части ОС.

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

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.

ALC_TAT_EXT.0 Определение инструментальных средств разработки

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_TAT_EXT.0.1D Заявитель (разработчик, производитель) должен идентифицировать инструментальные средства, использованные при разработке операционной системы.

ALC_TAT_EXT.0.2D Заявитель (разработчик, производитель) должен задокументировать опции инструментальных средств разработки, использованные при разработке операционной системы.

Элементы содержания и представления документированных материалов

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

ALC_TAT_EXT.0.2C В документированных материалах должны быть отражены опции инструментальных средств разработки, использованные при разработке операционной системы.

Элементы действий испытательной лаборатории

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

7.2.4. Оценка задания по безопасности (ASE)

ASE_CCL.1 Утверждения о соответствии

Зависимости: ASE_INT.1 Введение ЗБ;
ASE_ECD.1 Определение расширенных компонентов;
ASE_REQ.1 Установленные требования безопасности.

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления 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 ЗБ

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

ASE_INT.1.1C «Введение ЗБ» должно содержать «Ссылку на ЗБ», «Ссылку на ОО», «Аннотацию ОО» и «Описание ОО».

ASE_INT.1.2C «Ссылка на ЗБ» должна однозначно идентифицировать ЗБ.

ASE_INT.1.3C «Ссылка на ОО» должна однозначно идентифицировать ОО.

ASE_INT.1.4C В «Аннотации ОО» должна быть представлена краткая информация о его использовании и основных функциональных возможностях безопасности ОО.

ASE_INT.1.5C В «Аннотации ОО» должен быть идентифицирован тип ОО.

ASE_INT.1.6C В «Аннотации ОО» должны быть идентифицированы любые не входящие в ОО аппаратные, программные, а также программно-аппаратные средства, требуемые ОО.

ASE_INT.1.7C «Описание ОО» должно включать описание физических границ ОО.

ASE_INT.1.8C «Описание ОО» должно включать описание логических границ ОО.

Элементы действий испытательной лаборатории

ASE_INT.1.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_INT.1.1C – ASE_INT.1.8C.

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

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

ASE_OBJ.2 Цели безопасности

Зависимости: ASE_SPD.1 Определение проблемы безопасности.

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления документированных материалов

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

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

ASE_OBJ.2.3C В «Обосновании целей безопасности» каждая цель безопасности для **среды функционирования** должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, а также к предположениям, поддерживаемым данной целью безопасности.

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

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

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

Элементы действий испытательной лаборатории

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

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

ASE_REQ.2 Производные требования безопасности

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

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления документированных материалов

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

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

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

ASE_REQ.2.4C Все операции должны **быть выполнены** правильно.

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

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

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

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

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

Элементы действий испытательной лаборатории

ASE_REQ.2.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_REQ.2.1C – ASE_REQ.2.9C.

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

ASE_SPD.1 Определение проблемы безопасности

Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

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

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

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

Элементы действий испытательной лаборатории

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

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

ASE_TSS.1 Краткая спецификация ОО

Зависимости: ASE_INT.1 Введение ЗБ.

ASE_REQ.1 Установленные требования безопасности

ADV_FSP.1 Базовая функциональная спецификация

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

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

Элементы действий испытательной лаборатории

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

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

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

7.2.5. Тестирование (ATE)

ATE_COV.1 Свидетельство покрытия

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

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

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

Элементы действий испытательной лаборатории

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

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

ATE_FUN.1 Функциональное тестирование

Зависимости: ATE_COV.1 Свидетельство покрытия.

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления документированных материалов

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

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

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

ATE_FUN.1.4C Фактические результаты тестирования должны соответствовать ожидаемым.

Элементы действий испытательной лаборатории

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

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

ATE_IND.2 Выборочное независимое тестирование

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

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

ATE_IND.2.1C ОО должен быть пригоден для тестирования.

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

Элементы действий испытательной лаборатории

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

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

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

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

7.2.6. Оценка уязвимостей (AVA)

AVA_VAN.4 Методический анализ уязвимостей

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

Элементы действий заявителя (разработчика, производителя)

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

Элементы содержания и представления документированных материалов

AVA_VAN.4.1C **Документация анализа уязвимостей должна:**

а) содержать результаты анализа, выполненного для поиска способов, которыми потенциально может быть нарушена реализация ФТБ;

б) идентифицировать проанализированные предполагаемые уязвимости;

в) демонстрировать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

Элементы действий испытательной лаборатории

AVA_VAN.4.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AVA_VAN.4.1C.

AVA_VAN.4.2E Испытательная лаборатория должна выполнить поиск информации в общедоступных источниках **в целях идентификации потенциальных уязвимостей** в ОО.

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

AVA_VAN.4.4E Испытательная лаборатория должна провести тестирование проникновения, основанное на идентифицированных уязвимостях **в целях оформления заключения о стойкости ОО** к нападениям, выполняемым нарушителем, обладающим **умеренным** потенциалом нападения.

Замечания по применению:

1. В качестве общедоступных источников в первую очередь должна использоваться база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России.
2. Тесты проникновения должны быть направлены на тестирование уязвимостей, которые потенциально могут быть использованы нарушителем для обхода, отключения или преодоления функций безопасности ОО.

7.2.7. Требования к объекту оценки, сформулированные в явном виде

ALC_FPU_EXT.1 Процедуры обновления программного обеспечения операционной системы

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.

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность операционные системы

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 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 (разработчика, производителя)

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** внешних модулей уровня ядра ОС на безопасность ОС, 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, изложенным в AMA_SIA_EXT.6.1C, AMA_SIA_EXT.6.2C.

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

AVA_CCA_EXT.1 Анализ скрытых каналов

Элементы действий заявителя (разработчика, производителя)

AVA_CCA_EXT.1.1D Заявитель (разработчик, производитель) должен провести поиск скрытых каналов для реализуемых ОС ***политик управления доступом*** [выбор: *политики управления информационными потоками; ограничения по наблюдению за действиями пользователей ОС; [назначение: иные политики или ограничения]*, ***нет***].

AVA_CCA_EXT.1.2D Заявитель (разработчик, производитель) должен представить документацию по анализу скрытых каналов.

Элементы содержания и представления документированных материалов

AVA_CCA_EXT.1.1C В документации по анализу скрытых каналов должны быть идентифицированы скрытые каналы и содержаться оценка их пропускной способности.

AVA_CCA_EXT.1.2C Документация по анализу скрытых каналов должна содержать описание процедур, использованных для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

AVA_CCA_EXT.1.3C Документация по анализу скрытых каналов должна содержать описание всех предположений (быстродействие процессора, системная конфигурация, объем памяти и (или) иных), сделанных при анализе скрытых каналов.

AVA_CCA_EXT.1.4C Документация по анализу скрытых каналов должна содержать описание метода, использованного для оценки пропускной способности канала для наиболее опасного сценария.

AVA_CCA_EXT.1.5C Документация по анализу скрытых каналов должна содержать описание наиболее опасного сценария использования каждого идентифицированного скрытого канала.

Элементы действий испытательной лаборатории

AVA_CCA_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 AVA_CCA_EXT.1.1C - AVA_CCA_EXT.1.5C.

AVA_CCA_EXT.1.2E Испытательная лаборатория должна подтвердить, что результаты анализа скрытых каналов, выполненного заявителем (разработчиком, производителем), свидетельствуют об удовлетворении ОС соответствующих функциональных требований (по управлению информационными потоками, управлению доступом, предотвращению наблюдения одним пользователем за действием другого пользователя, предотвращению использования информационных потоков для распространения неразрешенных информационных сигналов, контролю и ограничению скрытых каналов и (или) иных).

AVA_CCA_EXT.1.3E Испытательная лаборатория должна подтвердить правильность результатов анализа скрытых каналов, выполненного заявителем (разработчиков, производителем).

Замечания по применению:

1. Поиск скрытых каналов (неразрешенных информационных потоков) проводится для типов скрытых каналов, определенных в национальном стандарте ГОСТ Р 53113.1 – 2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения» с учетом рекомендаций, изложенных в национальном стандарте ГОСТ Р 53113.2 – 2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов», и потенциала нарушителя.

2. Для предотвращения возникновения скрытых каналов в информационных системах (автоматизированных системах управления), связанных с применением ОО, для всех выявленных скрытых каналов в ОО (предпосылок возникновения скрытых каналов) с учетом рекомендаций, изложенных в национальном стандарте ГОСТ Р 53113.2 – 2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов», и потенциала нарушителя должны быть предусмотрены и включены в задание по безопасности:

соответствующие цели для среды функционирования ОО и (или);

функциональные требования безопасности, выраженные 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» (FDP_IFF.3-6 и (или) иных) и (или) специальных (расширенных) компонентов, и описание соответствующих механизмов, используемых ОО с целью ограничения, мониторинга, полного или частичного устранения скрытых каналов (неразрешенных информационных потоков).

7.3. Обоснование требований безопасности

7.3.1. Обоснование требований безопасности для объекта оценки

7.3.1.1. Обоснование функциональных требований безопасности объекта оценки

В таблице 7.4 представлено отображение функциональных требований безопасности на цели безопасности для ОО.

Таблица 7.4 – Отображение функциональных требований безопасности на цели безопасности

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8
FAU_GEN.1						X		
FAU_SEL.1						X		
FAU_SAR.1						X		
FAU_STG.1						X		
FAU_STG.3						X		
FAU_STG.4						X		
FDP_ACC.1(1)		X						
FDP_ACC.1(2)		X						
FDP_ACF.1(1)		X		X				
FDP_ACF.1(2)		X						
FDP_RIP.1					X			
FDP_RSI_EXT.1			X					
FDP_RSP_EXT.1			X					
FDP_RSP_EXT.2			X					
FIA_UAU.2	X							
FIA_UID.2	X							
FMT_MOF.1		X						
FMT_MSA.1(1)		X						
FMT_MSA.1(2)		X						
FMT_MTD.1	X							
FMT_SMF.1								X
FMT_SMR.1								X
FPT_APW_EXT.1	X							
FPT_MTR_EXT.1		X						
FPT_TST.1				X				
FPT_RCV.2				X				
FPT_STM.1							X	
FPO_DFS_EXT.1			X					
FPO_OBF_EXT.1			X					
FRU_PRS_EXT.3					X			

Включение указанных в таблице 7.4 функциональных требований безопасности ОО в ПЗ определяется Требованиями безопасности информации к операционным системам, утвержденными приказом ФСТЭК России от 19 августа 2016 г. № 119.

FAU_GEN.1 Генерация данных аудита

Выполнение требований данного компонента обеспечивает возможность регистрации возникновения всех событий, связанных с выполнением функций безопасности ОС, а также возможность полнотекстовой записи привилегированных команд (команд, управляющих системными функциями). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления администратору ОС всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, потенциально подвергаемых аудиту. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает возможность защиты хранимых записей аудита от несанкционированного удаления и предотвращение модификации записей аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_STG.3 Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает возможность защиты журнала аудита от переполнения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает возможность предотвращения потери данных аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FDP_ACC.1(1) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает возможность задания политики дискреционного метода управления доступом для определенного подмножества (списка, числа) операций, выполняемых субъектами доступа по отношению к объектам доступа. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FDP_ACC.1(2) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает возможность задания политики ролевого метода управления доступом для определенного подмножества (списка, числа) операций, выполняемых субъектами доступа по отношению к объектам доступа. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

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

Выполнение требований данного компонента обеспечивает возможность осуществления управления доступом к объектам доступа ОС на основе списков управления доступом или матрицы управления доступом. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2**, **Цель безопасности-4** и способствует их достижению.

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

Выполнение требований данного компонента обеспечивает возможность осуществления в ОС политики ролевого управления доступом для определенного подмножества (списка, числа) операций, выполняемых субъектами доступа по отношению к объектам доступа. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FDP_RIP.1 Ограниченная защита остаточной информации

Выполнение требований данного компонента обеспечивает обеспечение недоступности содержания остаточной информации назначенных ресурсов, контролируемых ОС, при распределении или освобождении ресурса. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FDP_RSI_EXT.1 Управление установкой программного обеспечения

Выполнение требований данного компонента обеспечивает управление установкой программного обеспечения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FDP_RSP_EXT.1 Правила запуска компонентов программного обеспечения

Выполнение требований данного компонента обеспечивает задание правил запуска компонентов программного обеспечения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FDP_RSP_EXT.2 Контроль запуска компонентов программного обеспечения

Выполнение требований данного компонента обеспечивает контроль запуска компонентов программного обеспечения в соответствии с правилами запуска. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает аутентификацию пользователя до выполнения любых действий по доступу в информационную систему или администратора до выполнения действий по управлению средством идентификации и аутентификации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает идентификацию пользователя до выполнения основных действий по доступу в информационную систему или администратора ОС до выполнения действий по управлению средством идентификации и аутентификации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_SMF.1 Спецификация функций управления

Выполнение требований данного компонента обеспечивает наличие у ОС, как минимум, функций управления режимом выполнения функций безопасности и функций управления данными ФБО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-8** и способствует ее достижению.

FMT_MOF.1 Управление режимом выполнения функций безопасности

Выполнение требований данного компонента обеспечивает разрешение ФБО на модификацию режима выполнения функций ОС администраторам ОС и другим уполномоченным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FMT_MSA.1(1) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FMT_MSA.1(2) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики ролевого управления доступом только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FMT_MTD.1 Управление данными функций безопасности

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

FMT_SMR.1 Роли безопасности

Выполнение требований данного компонента обеспечивает поддержание ролей безопасности и их ассоциации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-8** и способствует ее достижению.

FPT_MTR_EXT.1 Монитор обращений

Выполнение требований данного компонента обеспечивает постоянный контроль обращений субъектов доступа к объектам доступа, проверку правомочности обращений в соответствии с установленными политиками и правилами управления доступом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FPT_APW_EXT.1 Защита хранимой аутентификационной информации

Выполнение требований данного компонента обеспечивает возможность предотвращения хранения и чтения аутентификационной информации в открытом виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FPT_TST.1 Тестирование функциональных возможностей безопасности

Выполнение требований данного компонента обеспечивает возможность тестирования (самотестирования) функций безопасности ОС, проверки целостности программного обеспечения ОС и целостности данных ОС. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FPT_RCV.2 Автоматическое восстановление

Выполнение требований данного компонента обеспечивает возможность обеспечения восстановления штатного режима функционирования ОС. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Выполнение требований данного компонента обеспечивает возможность предоставления надежных меток времени при проведении аудита, а также для ограничения срока действий атрибутов безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FPO_DFS_EXT.1 Изоляция процессов

Выполнение требований данного компонента обеспечивает возможность обеспечения защиты от несогласованности возникающих на уровне процессов, при параллельной работе с объектами доступа. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FPO_OBF_EXT.1 Блокирование файлов процессами

Выполнение требований данного компонента обеспечивает возможность блокирования попыток несанкционированных действий над объектами доступа, если в момент обращения к объекту доступа он используется другим процессом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FRU_PRS_EXT.3 Приоритизация процессов

Выполнение требований данного компонента обеспечивает возможность приоритизации процессов. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

7.3.1.2.Обоснование удовлетворения зависимостей функциональных требований безопасности

В таблице 7.5 представлены результаты удовлетворения зависимостей функциональных требований безопасности. Все зависимости компонентов требований удовлетворены в настоящем профиле защиты либо включением компонентов, определенных в национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Часть 2. Функциональные компоненты безопасности» под рубрикой «Зависимости».

Столбец 2 таблицы 7.5 является справочным и содержит компоненты, определенные в национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» в описании компонентов требований, приведенных в столбце 1 таблицы 7.5, под рубрикой «Зависимости».

Столбец 3 таблицы 7.5 показывает, какие компоненты требований были включены в настоящий ПЗ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 7.5. Компоненты требований в столбце 3 таблицы 7.5 либо совпадают с компонентами в столбце 2 таблицы 7.5, либо иерархичны по отношению к ним.

Таблица 7.5 – Зависимости функциональных требований безопасности

Функциональный компонент	**Зависимость в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 7.1 настоящего ПЗ**	**Удовлетворение зависимости**
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 FMT_MTD.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.1
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	FDP_ACC.1	FDP_ACC.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_RCV.2	AGD_OPE.1	AGD_OPE.1

Компонент FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности», в том числе, имеет зависимости от компонентов FMT_MSA.3 «Инициализация статических атрибутов» и FMT_MSA.1 «Управление атрибутами безопасности».

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

7.3.2. Обоснование требований доверия к безопасности объекта оценки

Требования доверия настоящего ПЗ соответствуют ОУД2, усиленному компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_FLR.1 «Базовое устранение недостатков», AVA_VAN.4 «Методический анализ уязвимостей», расширенному компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_TAT_EXT.0 «Определение инструментальных средств разработки», 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов».

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

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 (изоляция 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: ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», 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» и AVA_CCA_EXT.1 «Анализ скрытых каналов», 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 ADV «Разработка»

Б.1.1. Реализация ОО (ADV_IMP_EXT.3)

Цели

Цель проверки выполнения требования ADV_IMP_EXT.3 заключается в обеспечении прослеживания реализации ОО к представлению реализации ФБО.

ADV_IMP_EXT.3 Реализация ОО

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_IMP.2 Полное отображение представления реализации ФБО.

Элементы действий заявителя (разработчика, производителя)

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

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

Элементы содержания и представления документированных материалов

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

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

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

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

Элементы действий испытательной лаборатории

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

Б.2. Класс ALC «Поддержка жизненного цикла»

Б.2.1. 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.2.2. 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.3. Класс AMA «Поддержка доверия»

Б.3.1. 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.

Б.4. Класс AVA «Оценка уязвимостей»

Б.4.1. Анализ скрытых каналов (AVA_CCA_EXT)

Цели

Анализ скрытых каналов является частью анализа уязвимостей и проводится с целью сделать заключение о существовании и потенциальной пропускной способности каналов передачи сигналов (коммуникационных каналов), которые не предусмотрены для передачи защищаемой информации (данных пользователя и иной информации) или неразрешенных сигналов, но которые могут быть для этого использованы потенциальными нарушителями (в нарушение установленных политик управления информационными потоками, управления доступом или иных установленных ограничений).

В качестве скрытых каналов рассматриваются:

каналы передачи, предназначенные для управления, но которые (в нарушение политики управления доступом или политики управления потоками) потенциально могут использоваться для передачи данных пользователя;

каналы передачи, предназначенные для передачи данных пользователя, но которые потенциально могут использоваться для передачи сигналов нарушителя (в том числе с использованием модуляции передачи данных);

каналы передачи, которые (в нарушение установленных ограничений) потенциально могут использоваться для наблюдения одним пользователем за действиями другого пользователя;

иные типы скрытых каналов.

AVA_CCA_EXT.1 Анализ скрытых каналов

Иерархический для: нет подчиненных компонентов.

Зависимости: AVA_VAN.4 Методический анализ уязвимостей;
ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации;
ADV_IMP.2 Полное отображение представления реализации функций безопасности объекта оценки;
AGD_OPE.1 Руководство пользователя по эксплуатации;
AGD_PRE.1 Подготовительные процедуры;
[FDP_ACC.1 Ограниченное управление доступом
или
FDP_IFC.1 Ограниченное управление информационными потоками,
или
FPR_UNO.1 Скрытность].

Элементы действий заявителя (разработчика, производителя)

AVA_CCA_EXT.1.1D Заявитель (разработчик, производитель) должен провести поиск скрытых каналов для реализуемых операционной системой [выбор: *политики управления информационными потоками; политики управления доступом, ограничения по наблюдению за действиями пользователей; [назначение: иные политики или ограничения]*].

AVA_CCA_EXT.1.2D Заявитель (разработчик, производитель) должен представить документацию по анализу скрытых каналов.

Элементы содержания и представления документированных материалов

AVA_CCA_EXT.1.1C В документации по анализу скрытых каналов должны быть идентифицированы скрытые каналы и содержаться оценка их пропускной способности.

AVA_CCA_EXT.1.2C Документация по анализу скрытых каналов должна содержать описание процедур, использованных для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

AVA_CCA_EXT.1.3C Документация по анализу скрытых каналов должна содержать описание всех предположений (быстродействие процессора, системная конфигурация, объем памяти и (или) иных), сделанных при анализе скрытых каналов.

AVA_CCA_EXT.1.4C Документация по анализу скрытых каналов должна содержать описание метода, использованного для оценки пропускной способности канала для наиболее опасного сценария.

AVA_CCA_EXT.1.5C Документация по анализу скрытых каналов должна содержать описание наиболее опасного сценария использования каждого идентифицированного скрытого канала.

Элементы действий испытательной лаборатории

AVA_CCA_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 AVA_CCA_EXT.1.1C - AVA_CCA_EXT.1.5C.

AVA_CCA_EXT.1.2E Испытательная лаборатория должна подтвердить, что результаты анализа скрытых каналов, выполненного заявителем (разработчиком, производителем), свидетельствуют об удовлетворении операционной системой соответствующих функциональных требований (по управлению информационными потоками, управлению доступом, предотвращению наблюдения одним пользователем за действием другого пользователя, предотвращению использования информационных потоков для распространения неразрешенных информационных сигналов, контролю и ограничению скрытых каналов и (или) иных).

AVA_CCA_EXT.1.3E Испытательная лаборатория должна подтвердить правильность результатов анализа скрытых каналов, выполненного заявителем (разработчиков, производителем).

Формат 60х90/8. Усл.печ.л. 13,25
Зак. 67
2017 г.