Серверная операционная система с интегрированными серверными службами МСВСфера 7.3 Сервер

Задание по безопасности МСВСфера7.3_Сервер_ЗБ

Версия 1.0

Содержание

Перечень сокращений

ACL	Access control list (Список контроля доступа)
AIDE	Advanced Instrusion Detection Environmnt (Среда обнаружения вторжений)
GID	Group Identifier (Идентификатор группы)
DAC	Discretionary access control (Дискреционное управление доступом)
ID	Identifier (Идентификатор)
LAF	Lightweight audit framework (Платформа аудита)
LDAP	Lightweight Directory Access Protocol (Протокол доступа к каталогам)
MLS	Multilevel security (Многоуровневая система безопасности)
NIS	Network Information Service (Информационная служба сети)
PAM	Pluggable Authentication Module (Модуль аутентификации)
PIC	Position-Independent Code (Позиционно независимый код)
PIE	Position-Independent Execution (Позиционно независимая программа)
PID	Process identifier (Идентификатор процесса)
SELinux	Security-enhanced Linux (Linux с улучшенной безопасностью)
SSH	Secure shell (Безопасная оболочка)
SSL	Secure socets layer (Уровень защищенных сокетов)
RBAC	Role-based access control (Управление доступом на основе ролей)
RPM	RPM Package Manager (Система управления пакетами в формате RPM)
ЗБ	Задание по безопасности
ИС	Информационная система
ИТ	Информационная технология
ИФБО	Интерфейс ФБО
ОДФ	Область действия ФБО
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
ФБ	Функция безопасности
ФБО	Функциональные возможности безопасности ОО
ФТБ	Функциональные требования безопасности к ОО

1 Введение

1.1 Ссылка на ЗБ

Название ЗБ:	Серверная операционная система с интегрированными серверными службами МСВСфера 7.3 Сервер. Задание по безопасности
Версия ЗБ:	1.0
Обозначение ЗБ:	МСВСфера7.3_Сервер_ЗБ
Разработчик ЗБ:	ООО «Национальный центр поддержки и разработки»
Дата выпуска ЗБ:	28 ноября 2020 года

1.2 Ссылка на ОО

Разработчик ОО:	ООО «Национальный центр поддержки и разработки»
Название ОО:	Серверная операционная система с интегрированными серверными службами МСВСфера 7.3 Сервер
Версия ОО:	7.3
Обозначение ОО:	МСВСфера 7.3 Сервер

1.3 Аннотация ОО

1.3.1 Использование и основные характеристики безопасности ОО

Настоящий документ определяет требования по безопасности для оценки серверной операционной системы с интегрированными серверными службами МСВСфера 7.3 Сервер в базовой конфигурации (далее – объект оценки, ОО).

ОО представляет собой многопользовательскую многозадачную операционную систему (ОС), относящуюся к классу высокопроизводительных отказоустойчивых ОС на базе ядра Linux, ориентированных на поддержку разнообразных серверных приложений.

ОО может использоваться для работы на автономном компьютере, в сетевом окружении с другими экземплярами ОО, а также с иными совместимыми системами одного управляемого домена, сконфигурированными в соответствии с общей политикой безопасности.

Имеющиеся в ОО средства обеспечения безопасности реализуют функции, включающие: идентификацию и аутентификацию, управление доступом, регистрацию событий безопасности, ограничение программной среды, изоляцию процессов, защиту памяти, контроль целостности, обеспечение надежного функционирования, фильтрацию сетевого потока.

1.3.2 Тип ОО

ОО относится к типу универсальных ОС, предназначенных для функционирования на средствах вычислительной техники, относящихся к классу серверов общего назначения (ОО относится к ОС типа «А»).

1.3.3 Требуемые аппаратные средства и программное обеспечение, не входящие в ОО

ОО предназначен для функционирования на 64-разрядных аппаратных платформах Intel/AMD и поддерживает использование многими пользователями одного или более процессоров и присоединенных внешних устройств, таких, как запоминающие устройства, устройства печати, мониторы, манипуляторы типа «мыш», клавиатуры, сетевые адаптеры. При этом, ОО не включает ни аппаратные средства, ни пограничное между ОО и аппаратными средствами предустановленное программное обеспечение микропрограммного уровня, которые являются частью среды функционирования ОО.

1.4 Описание ОО

1.4.1 Физические границы ОО

ОО поставляется в виде верифицированного ISO-образа инсталляционного дистрибутива вместе с эксплуатационной документацией, включающей руководство администратора, руководство пользователя, задание по безопасности и формуляр в котором изложены условия, ограничения и требования по эксплуатации.

Поставка может осуществляться с помощью почтовой и/или курьерской служб на оптических дисках, упакованных в футляры, опечатанные специальными защитными стикерами, а также по общедоступным каналам связи из специального защищенного репозитория в подписанном усиленной квалифицированной подписью виде.

1.4.2 Логические границы ОО

В состав ОО 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.

Логические границы ОО определяются функциями безопасности, которые реализуются процессами ядра и другими доверенными процессами, и могут быть кратко описаны нижеследующим образом.

1.4.2.1 Идентификация и аутентификация

Средства, реализующие данную функцию, обеспечивают: идентификациию и аутентификацию пользователей, устройств, объектов

файловых систем, запускаемых и исполняемых модулей; управление идентификаторами, в том числе создание, присвоение, уничтожение; управление параметрами аутентификации, в том числе создание, хранение, выдача, блокирование, разблокирование; возможность использования различных методов аутентификации: парольной аутентификации и SSH-аутентификации и их сочетаний; возможность устанавливать сроки действия идентификаторов и параметров аутентификации; защиту хранимой аутентификационной информации, исключение отображения действительного значения аутентификационной информации при ее вводе в диалоговом интерфейсе; возможность проверки соответствия аутентификационной информации заданной метрике качества; возможность устанавливать пороговое значение количества неуспешных попыток аутентификации и блокировать доступ пользователя при его превышении; возможность ассоциировать атрибуты безопасности пользователя с запускаемыми от его имени процессами.

1.4.2.2 Управление доступом

Средства, реализующие данную функцию, обеспечивают: возможность ограничивать доступ пользователя к ОО в запрещенные периоды времени, а также ограничивать для него количество одновременно предоставляемых параллельных сеансов доступа; возможность завершения, блокирования и разблокирования сеанса доступа путем повторной аутентификации по инициативе самого пользователя, по требованию уполномоченного привилегированного субъекта доступа или по истечению заданного для пользователя так называемого времени бездействия; возможность задания и реализации политик дискреционного и ролевого управления доступом субъектов доступа к объектам доступа на основе списков управления доступом и ролей; поддержку определенных ролей и их ассоциации с пользователями; постоянный контроль и проверку правомочности обращений субъектов доступа к объектам доступа; защиту от несогласованностей, возникающих на уровне процессов при параллельной работе с ресурсами средств вычислительной техники и объектами доступа; возможность блокирования попыток доступа субъектов доступа к объектам доступа, если в момент обращения они используются другими субъектами; возможность назначения приоритетов для использования субъектами доступа подмножества вычислительных ресурсов средства вычислительной техники; возможность квотирования предоставляемых вычислительных ресурсов.

1.4.2.3 Регистрация событий безопасности

Средства, реализующие данную функцию, обеспечивают: возможность регистрации событий безопасности; включения и исключения событий в совокупность событий, подлежащих регистрации, и предоставления всей регистрируемой информации в понятном виде; возможность защиты хранимых записей регистрации событий безопасности от несанкционированного удаления и модификации; возможность выполнения действий, направленных на сохранение данных журнала регистрации событий безопасности и

обеспечивающих непрерывность процесса регистрации при превышении журналом регистрации определенного размера, возможность поиска, выборочного просмотра, сортировки и упорядочения данных регистрации; возможность передавать данные регистрации для внешнего хранения.

1.4.2.4 Ограничение программной среды

Средства, реализующие данную функцию, обеспечивают: возможность применения наборов базовых конфигураций ОС; возможность установки компонентов ПО доверенным образом и задания правил их автоматического запуска при загрузке ОС, а также правил запуска в процессе функционирования ОС; контроль запуска и реагирование на попытки запуска компонентов ПО, произведенные в нарушение установленных правил; контроль целостности разрешенных для запуска компонентов ПО и реагирование на попытки запуска компонентов, целостность которых была нарушена; обеспечение защиты от переполнения буфера.

1.4.2.5 Изоляция процессов

Средства, реализующие данную функцию, обеспечивают возможность безопасного выделения процессам областей оперативной памяти; защиту от несогласованностей, возникающих на уровне процессов при параллельной работе с областями памяти, файлами и устройствами.

1.4.2.6 Защита памяти

Средства, реализующие данную функцию, обеспечивают недоступность остаточной информации при распределении или освобождении ресурса памяти, а также возможность удаления объектов файловой системы, в том числе путем многократной перезаписи специальными битовыми последовательностями.

1.4.2.7 Контроль целостности

Средства, реализующие данную функцию, обеспечивают возможность тестирования функций безопасности ОО, проверки целостности ПО и целостности данных ОО, а также контроль целостности компонентов ПО, разрешенного для запуска.

1.4.2.8 Обеспечение надежного функционирования

Средства, реализующие данную функцию, обеспечивают: возможность предоставления надежных меток времени; возможность резервного копирования объектов файловой системы; возможность возврата ОС при сбоях и отказах к безопасному состоянию в ручном и автоматизированном режиме; возможность восстановления объектов ОС из созданных с использованием ОС резервных копий и использования ассоциированных с ними атрибутов безопасности; возможность работы отдельных экземпляров ОС на нескольких

технических средствах в отказоустойчивом режиме, обеспечивающем доступность сервисов и информации при выходе из строя одного из технических средств или при исчерпании предоставляемых вычислительных ресурсов.

1.4.2.9 Фильтрация сетевого потока

Средства, реализующие данную функцию, обеспечивают: возможность осуществлять фильтрацию входящих и (или) исходящих сетевых потоков, базируясь на устанавливаемом наборе правил фильтрации сетевого трафика, основанном на идентифицированных атрибутах безопасности субъектов доступа и сетевых протоколах транспортного и прикладного уровня; возможность управлять правилами фильтрации сетевого потока; возможность регистрации и учета выполнения проверок при фильтрации сетевого потока.

2. Утверждения о соответствии

2.1 Утверждение о соответствии ГОСТ Р ИСО/МЭК 15408

Настоящее ЗБ основано на комплексе национальных стандартов Российской Федерации: ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».

2.2 Утверждение о соответствии ПЗ

Настоящее ЗБ разработано в соответствии с методическим документом ФСТЭК России «Профиль защиты операционных систем типа «А» четвертого класса защиты» (Профиль защиты ИТ.ОС.А4.ПЗ), утвержденным 8 февраля 2017 года, использует определенные в нем понятия и не добавляет по отношению к нему угроз безопасности, политик безопасности, предположений безопасности и функциональных требований безопасности.

Исходя из особенностей ОО при формулировании требований безопасности в настоящем ЗБ применены следующие соглашения по форматированию текста:

жирным шрифтом обозначаются идентификаторы и названия компонентов требований безопасности, а также необходимые текстуальные уточнения их определений;

порядковым номером в круглых скобках вслед за идентификатором компонента требований безопасности обозначается его повторное использование с целью охвата различных аспектов одного и того же требования;

жирным шрифтом в квадратных скобках обозначается назначение, позволяющее специфицировать заданный параметр компонента требований безопасности;

жирным курсивом в квадратных скобках обозначается выбор, позволяющий специфицировать один или несколько элементов из списка параметров компонента требований безопасности.

2.3 Утверждение о соответствии пакетам

Настоящее ЗБ соответствует требованиям к разработке и производству, проведению испытаний и поддержке безопасности средства, соответствующего 4 уровню доверия согласно документу «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденному приказом ФСТЭК России от 2 июня 2020 г. № 76.

2.4 Обоснование соответствия

Включение функциональных требований и требований доверия к ОО в настоящее ЗБ определяется «Требованиями безопасности информации к операционным системам», утвержденными приказом ФСТЭК России от 19 августа 2016 г. № 119, и «Требованиями по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденными приказом ФСТЭК России от 2 июня 2020 г. № 76, соответственно.

3. Определение проблемы безопасности

Данный раздел содержит определение проблемы безопасности, а именно:

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

политик безопасности, которые должны быть реализованы ОО, его средой функционирования или их сочетанием,

предположений безопасности, определяющих обязательные условия безопасного использования ОО.

Представленное здесь определение проблемы безопасности согласуется с определением проблемы безопасности в вышеупомянутом Профиле защиты ИТ.ОС.А4.ПЗ.

3.1 Угрозы

3.1.1 Угрозы, которым должен противостоять 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 – получение нарушителем несанкционированного доступа к информации, обрабатываемой средством вычислительной техники, в период, когда пользователь ОС покинул рабочее место, не завершив сеанс работы в ОС.
2. Источники угрозы – внутренний нарушитель.
3. Способ реализации угрозы – некорректное завершение сеанса доступа пользователя ОС.

4. Используемые уязвимости – недостатки механизмов управления доступом, связанные с защитой сеанса пользователя ОС.

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

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

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

Угроза-3

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-4

1. Аннотация угрозы – несанкционированное или непреднамеренное 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-5

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 оперативной памяти, используемой процессами и формируемыми ими потоками данных, или к сегментам 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-6

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-7

1. Аннотация угрозы – осуществление нарушителем 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 в части задания характеристик аутентификационной информации и ограничений по вводу; 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-8

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 файловой системы и устройствам 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-9

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-10

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-11

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- 12

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.

3.1.2 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.
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 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.

3.2 Политики безопасности, которые должны быть реализованы

Политика безопасности-1

Должны использоваться механизмы идентификации (однозначная идентификация пользователей ОС по используемым ими уникальным идентификаторам, ассоциация атрибутов безопасности пользователя ОС с субъектами доступа (процессы, потоки данных), действующими от имени этого пользователя ОС) и аутентификации (подтверждение подлинности пользователя ОС, ограничение неуспешных попыток аутентификации, защита вводимой пользователем ОС в диалоговом интерфейсе аутентификационной информации) пользователей ОС.

Политика безопасности-2

Должно осуществляться управление идентификаторами пользователей ОС (присвоение и блокирование идентификаторов, а также ограничение срока действия идентификаторов (учетных записей) пользователей ОС).

Политика безопасности-3

Должно осуществляться управление средствами аутентификации пользователей ОС (создание и присвоение аутентификационной информации, проверка требований к параметрам аутентификационной информации, смена пользователями ОС собственной аутентификационной информации (включая начальную аутентификационную информацию), а также ограничение срока

действия аутентификационной информации), а также защита хранимой аутентификационной информации.

Политика безопасности-4

Должна обеспечиваться возможность идентификации объектов файловой системы с целью обеспечения применения результатов идентификации при реализации в ОС механизмов управления доступом, контроля целостности, резервного копирования и регистрации событий безопасности, связанных с этими объектами.

Политика безопасности-5

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, устройствам) должно быть реализовано дискреционное и ролевое управление доступом.

Политика безопасности-6

Должна осуществляться возможность задания правил управления доступом, разрешающих или запрещающих доступ субъектов доступа к объектам доступа (объектам файловой системы, записям реестра, устройствам), 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; модификацию данных в объекте файловой системы, чтение информации из объекта файловой системы, запуск исполняемых объектов файловой системы, установка компонентов программного обеспечения, использование устройства) с использованием атрибутов безопасности объектов доступа и субъектов доступа на основе реализованных в ОС методов управления доступом (дискреционный, ролевой).

Политика безопасности-7

Должны осуществляться ограничение числа параллельных сеансов и контроль доступа в ОС с учетом параметров, связанных со временем доступа пользователей ОС (временем работы под учетной записью пользователя ОС) в ОС, а также своевременное завершение сеанса взаимодействия пользователя ОС с ОС по истечении определенного администратором времени бездействия.

Политика безопасности-8

Должна обеспечиваться возможность генерирования надежных меток времени.

Политика безопасности-9

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-10

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

Политика безопасности-11

Должна обеспечиваться возможность резервного копирования объектов файловой системы и компонентов ОС.

Политика безопасности-12

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-13

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-14

Должна обеспечиваться возможность применения наборов базовых конфигураций ОС.

Политика безопасности-15

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

Политика безопасности-16

Должны быть обеспечены регистрация возможных нарушений безопасности и предупреждение (сигнализация) о таких событиях. Механизмы регистрации должны предоставлять администратору возможность выборочного ознакомления с информацией о произошедших событиях.

Политика безопасности-17

Должны осуществляться контроль и фильтрация входящих и (или) исходящих сетевых потоков в соответствии с заданными правилами фильтрации сетевого потока. Должно обеспечиваться управление режимами выполнения и правилами фильтрации сетевого потока.

Политика безопасности-18

Должны обеспечиваться контроль установки и контроль запуска компонентов программного обеспечения.

Политика безопасности-19

Должны обеспечиваться: доступность сервисов и информации; возможность выделения вычислительных ресурсов для процессов в соответствии с их приоритетами.

Политика безопасности-20

Должна обеспечиваться защита от выполнения произвольного машинного кода.

Политика безопасности-21

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

3.3 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 совместимости ОС с СВТ 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) документацией.

Предположение-6

Должна обеспечиваться возможность генерации аутентификационной информации соответствующей метрике качества.

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.

Предположение, связанное с персоналом среды функционирования

Предположение-9

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

4. Цели безопасности

Данный раздел содержит определение целей безопасности для ОО и целей безопасности для среды функционирования ОО, а также обоснование, показывающее, что, если все цели безопасности будут достигнуты, то всем угрозам будет обеспечено противостояние, все политики безопасности будут реализованы и все предположения безопасности будут осуществлены, т.е. проблема безопасности будет решена.

Представленное здесь определение и обоснование целей безопасности согласуется с определением и обоснованием целей безопасности в вышеупомянутом Профиле защиты ИТ.ОС.А4.ПЗ.

4.1 Цели 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;

управление идентификаторами пользователей ОС и средствами аутентификации пользователей ОС для исключения возможности восстановления (подбора) аутентификационной информации пользователей ОС нарушителем и неправомерного доступа в ОС;

идентификацию объектов файловой системы для обеспечения применения результатов идентификации при реализации в ОС механизмов управления доступом, контроля целостности, резервного копирования и регистрации событий безопасности, связанных с этими объектами доступа.

Цель безопасности-2
Управление доступом

ОО должен обеспечивать:

дискреционное и ролевое управление доступом субъектов доступа (пользователей ОС и процессов, запускаемых от имени пользователей ОС) к объектам доступа в ОС (объектам файловой системы, записям реестра) 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;

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

Цель безопасности-3

Защита от несанкционированного доступа в обход правил управления доступом

ОО должен обеспечивать:

возможность ограничения числа параллельных сеансов и контроля доступа в ОС с учетом параметров, связанных со временем доступа пользователей ОС (временем работы под учетной записью пользователя ОС) в ОС, а также – своевременного завершения сеанса взаимодействия пользователя ОС с ОС по истечении определенного администратором времени бездействия для исключения возможности получения нарушителем несанкционированного доступа к информации, обрабатываемой средством вычислительной техники, в период, когда пользователь ОС покинул рабочее место, не завершив сеанс работы в ОС;

возможность очистки остаточной информации в памяти средства вычислительной техники при ее освобождении (распределении) или блокирования доступа субъектов доступа к остаточной информации 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 от выполнения произвольного машинного кода.

Цель безопасности-4

Обеспечение целостности, восстановления и резервного копирования 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 резервного копирования объектов файловой системы и компонентов ОС для исключения возможности утраты информации вследствие несанкционированного или непреднамеренного удаления информации со средства вычислительной техники, функционирующего под управлением ОС;

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
Фильтрация сетевого потока

ОО должен обеспечивать:

возможность контроля и фильтрации сетевого потока в соответствии с заданными правилами фильтрации входящих и (или) исходящих сетевых потоков;

возможность управления режимами выполнения и правилами фильтрации сетевого потока.

Цель безопасности-7
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-8
Генерирование временных меток

ОО должен обеспечивать генерирование надежных меток времени.

Цель безопасности-9
Управление ОС

ОО должен обеспечивать:

возможность применения наборов базовых конфигураций ОС;

возможность управления работой ОС и параметрами ОС со стороны администраторов.

4.2 Цели безопасности для среды функционирования ОО

В настоящем ЗБ определение целей безопасности для среды функционирования ОО согласуется с определением целей безопасности для среды функционирования ОО в вышеупомянутом Профиле защиты ИТ.ОС.А4.ПЗ, а именно:

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 неразрешенного 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 за пределы 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 осуществляться 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 в соответствии с их приоритетами.

Цель для среды функционирования ОО-13

Требования к персоналу-1

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

Цель для среды функционирования ОО-14
Требования к персоналу-2

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

Цель для среды функционирования ОО-15
Генерация аутентификационной информации

Должна обеспечиваться возможность генерации аутентификационной информации соответствующей метрике качества.

4.3 Обоснование целей безопасности

4.3.1 Обоснование целей безопасности для ОО

В настоящем ЗБ обоснование целей безопасности для ОО совпадает с аналогичным обоснованием целей безопасности для ОО вышеупомянутого профиля защиты ИТ.ОС.А4.ПЗ. Ниже в Таблице 4.1 представлено сопоставление целей безопасности для ОО с угрозами безопасности, которым должен противостоять ОО, и политиками безопасности. Оно демонстрирует, что каждая цель сопоставлена, по крайней мере, с одной угрозой или политикой безопасности, и что все угрозы, которым должен противостоять ОО, и политики безопасности надлежащим образом учтены в целях безопасности для ОО.

Таблица 4.1 – Отображение целей безопасности для ОО на угрозы и политики безопасности.

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

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9
Угроза – 9		X					X		
Угроза – 10			X						
Угроза – 11			X						
Угроза – 12					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				X					
Политика безопасности-13				X					
Политика безопасности-14									X
Политика безопасности-15									X
Политика безопасности-16							X		
Политика безопасности-17						X			
Политика безопасности-18			X						
Политика безопасности-19					X				
Политика безопасности-20			X						
Политика безопасности-21		X							

Цель безопасности-1

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-7, Угроза-8** и реализацией политик безопасности **Политика безопасности-1, Политика безопасности-2, Политика безопасности-3, Политика безопасности-4,** так как обеспечивает: использование механизмов идентификации и аутентификации пользователей ОС; управление идентификаторами пользователей ОС, в том числе присвоение и блокирование идентификаторов; управление средствами аутентификации пользователей ОС, в том числе создание, присвоение и смену начальной аутентификационной информации, а также периодическую и принудительную смену значений аутентификационной информации; возможность идентификации объектов ОС с целью обеспечения применения результатов

идентификации при реализации в ОС механизмов управления доступом, контроля целостности, резервного копирования и регистрации событий безопасности, связанных с этими объектами.

Цель безопасности-2

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-6**, **Угроза-9** и реализации политик безопасности **Политика безопасности-5, Политика безопасности-6**, **Политика безопасности-21,** так как обеспечивает: дискреционное и 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-2, Угроза-5, Угроза-10, Угроза-11** и реализации политик безопасности **Политика безопасности-7, Политика безопасности-9, Политика безопасности-10, Политика безопасности-18, Политика безопасности-20,** так как обеспечивает: возможность ограничения числа параллельных сеансов и контроля доступа в ОС с учетом параметров, связанных со временем доступа пользователей ОС; возможность очистки остаточной информации в памяти средства вычислительной техники при ее освобождении (распределении) или блокирование доступа субъектов доступа к остаточной информации; 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-4, Угроза-5** и реализации политик безопасности **Политика безопасности-11, Политика безопасности-12, Политика безопасности-13,** так как обеспечивает: возможность резервного копирования объектов файловой системы и компонентов ОС; 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-3**, **Угроза-12** и реализации политики безопасности **Политика**

безопасности-19, так как обеспечивает выделение вычислительных ресурсов в соответствии с приоритетами.

Цель безопасности-6

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-17,** так как обеспечивает возможность фильтрации входящих и (или) исходящих сетевых потоков в соответствии с заданными правилами фильтрации.

Цель безопасности-7

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-9** и реализации политики безопасности **Политика безопасности-16,** так как обеспечивает возможность регистрации и предупреждения (сигнализацию) о событиях, относящихся к возможным нарушениям безопасности.

Цель безопасности-8

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-8,** так как обеспечивает возможность генерирования меток времени и (или) синхронизации системного времени.

Цель безопасности-9

Достижение этой цели безопасности необходимо для реализации политик безопасности **Политика безопасности-14, Политика безопасности-15,** так как обеспечивает возможность применения наборов базовых конфигураций ОС и возможность управления работой ОС и параметрами ОС со стороны администраторов.

4.3.2 Обоснование целей безопасности для среды функционирования ОО

Ниже в Таблице 4.2 представлено сопоставление целей безопасности для среды функционирования ОО с угрозами безопасности, которым должна противостоять среда функционирования ОО, политиками безопасности и предположениями безопасности. Оно демонстрирует, что каждая цель для среды сопоставлена, по крайней мере, с одной угрозой для среды, политикой или предположением безопасности, и что все угрозы, которым должна противостоять среда функционирования ОО, и предположения безопасности надлежащим образом учтены в целях безопасности для среды функционирования ОО.

Таблица 4.2 – Отображение целей для среды на угрозы для среды, политики и предположения безопасности.

	Цель для среды-1	Цель для среды-2	Цель для среды-3	Цель для среды-4	Цель для среды-5	Цель для среды-6	Цель для среды-7	Цель для среды-8	Цель для среды-9	Цель для среды-10	Цель для среды-11	Цель для среды-12	Цель для среды-13	Цель для среды-14	Цель для среды-15
Угроза для среды-1				X											
Угроза для среды-2				X					X						
Угроза для среды-3			X												
Угроза для среды-4														X	
Угроза для среды-5						X									
Угроза для среды-6					X										
Угроза для среды-7						X									
Политика-1															
Политика-2															
Политика-3															X
Политика-4															
Политика-5															
Политика-6															
Политика-7															
Политика-8															
Политика-9										X					
Политика-10															
Политика-11					X										
Политика-12															
Политика-13				X											
Политика-14															
Политика-15							X	X							
Политика-16															
Политика-17															
Политика-18						X									
Политика-19												X			
Политика-20															
Политика-21										X					
Предположение-1			X												
Предположение-2	X														
Предположение-3		X				X									
Предположение-4		X													
Предположение-5				X							X				
Предположение-6															X
Предположение-7				X											
Предположение-8						X									
Предположение-9		X											X	X	

Цель для среды-1

Достижение этой цели необходимо для осуществления **Предположения-2,** так как обеспечивает условия совместимости ОО с СВТ, в которых он функционирует, для реализации своих возможностей.

Цель для среды-2

Достижение этой цели необходимо для осуществления **Предположения-3, Предположения-4** и **Предположения-9,** так как обеспечивает установку, конфигурирование, эксплуатацию и управление ОО ответственным за функционирование персоналом в соответствии с эксплуатационной документацией (правилами по безопасной настройке, руководствами пользователя и администратора), и тем самым обеспечивает невозможность несанкционированного внесения изменений в логику функционирования ОО через механизм обновления программного обеспечения ОО.

Цель для среды-3

Достижение этой цели необходимо для противостояния **Угрозе для среды-3** и осуществления **Предположения-1,** так как обеспечивает защиту от осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует ОО, и целостности данных, в том числе параметров настройки средств защиты информации ОО.

Цель для среды-4

Достижение этой цели необходимо для противостояния **Угрозе для среды-1** и **Угрозе для среды-2,** реализации **Политики-13,** осуществления **Предположения-5** и **Предположения-7,** так как обеспечивает: доверенную загрузку ОС, блокирование попыток отключения и/или обхода компонентов ОС, реализующих функции безопасности, путем подмены загружаемой ОС, контроль целостности программных компонентов загружаемой ОС, получаемых от поставщика.

Цель для среды-5

Достижение этой цели необходимо для противостояния **Угрозе для среды-6** и реализации **Политики-12,** так как обеспечивает необходимые ресурсы для выполнения функциональных возможностей безопасности ОС, хранение резервных копий, создаваемых ОС, защищенное хранение данных ОС и защищаемой информации, восстановление функциональных возможностей, настроек безопасности и штатного режима функционирования ОС при сбоях и ошибках.

Цель для среды-6

Достижение этой цели необходимо для противостояния **Угрозе для среды-5** и **Угрозе для среды-7,** реализации **Политики-18,** осуществления **Предположения-3** и **Предположения-8,** так как обеспечивает ограничение на установку программного обеспечения и его компонентов, не задействованных в технологическом процессе обработки информации, контроль установки и запуска компонентов программного обеспечения, блокирует несанкционированное внесение изменений в логику функционирования ОС через механизм обновления программного обеспечения ОС, блокирует несанкционированное внесение изменений в журналы регистрации событий безопасности с использованием специальных программных средств, обеспечивает недопущение снижения производительности ОС из-за внедрения в нее избыточного программного обеспечения.

Цель для среды-7

Достижение этой цели необходимо для реализации **Политики-15,** так как обеспечивает доверенный маршрут между ОС и ее пользователями, т.е возможности по управлению работой ОС и параметрами ОС со стороны администраторов.

Цель для среды-8

Достижение этой цели необходимо для реализации **Политики-15,** так как обеспечивает доверенный канал передачи данных между ОС и СВТ, на которых происходит обработка информации и с которых происходит их администрирование, т.е возможности по управлению работой ОС и параметрами ОС со стороны администраторов.

Цель для среды-9

Достижение этой цели необходимо для противостояния **Угрозе для среды-2,** так как обеспечивает невозможность отключения (обхода) компонентов ОС, реализующих функции безопасности.

Цель для среды-10

Достижение этой цели необходимо для противостояния **Угрозе для среды-6,** так как обеспечивает меры, препятствующие несанкционированному копированию информации, содержащейся в ОС, на съемные машинные носители.

Цель для среды-11

Достижение этой цели безопасности необходимо для осуществления **Предположения-5,** так как обеспечивает контроль целостности внешних модулей уровня ядра ОС, получаемых от поставщика.

Цель для среды-12

Достижение этой цели безопасности необходимо для реализации **Политики-19,** так как обеспечивает выделение вычислительных ресурсов для процессов в соответствии с их приоритетами и, тем самым, доступность сервисов и информации.

Цель для среды-13

Достижение этой цели необходимо для осуществления **Предположения-9,** так как обеспечивает точное соответствие действий персонала, ответственного за функционирование ОС, правилам и требованиям эксплуатационной документации.

Цель для среды-14

Достижение этой цели необходимо для противостояния **Угрозе для среды-4,** так как обеспечивает недоступность аутентификационной информации пользователей для лиц, не уполномоченных на доступ к ней.

Цель для среды-15

Достижение этой цели необходимо для реализации **Политики-3** и осуществления **Предположения-6,** так как обеспечивает возможность генерации аутентификационной информации соответствующей заданной метрике качества.

5. Определение расширенных компонентов

В настоящем ЗБ перечень и определение расширенных компонентов функциональных требований безопасности для ОО совпадает с перечнем и определением расширенных компонентов функциональных требований безопасности Профиля защиты ИТ.ОС.А4.ПЗ, а именно: FDP_CRC_EXT.1 «Восстановление информации», FDP_DDM_EXT.1 «Уничтожение (стирание) 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_OID_EXT.1 «Идентификация объектов доступа», FMT_UST_EXT.1 «Поддержка наборов базовых конфигураций», FPO_DFS_EXT.1 «Изоляция процессов», FPO_OBF_EXT.1 «Блокирование файлов процессами», FPO_RIP_EXT.1 «Безопасное выделение областей оперативной памяти», FPT_ACF_EXT.1 «Управление доступом к компонентам операционной системы», FPT_BOP_EXT.1 «Защита от переполнения буфера», FPT_MTR_EXT.1 «Монитор обращений», FPT_APW_EXT.1 «Защита хранимой аутентификационной информации».

6. Требования безопасности

В данном разделе определены требования безопасности для ОО, включающие функциональные требования безопасности и требования доверия к безопасности, которые должны быть выполнены, чтобы достигнуть сформулированных выше целей безопасности для ОО, и которые согласуются с требованиями безопасности для ОО, опредеденными в Профиле защиты ИТ.ОС.А4.ПЗ и с требованиями 4 уровня доверия, определенными в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденном приказом ФСТЭК России от 2 июня 2020 г. № 76.

Здесь представлено также сопоставление функциональных требований безопасности для ОО с ранее сформулированными целями безопасности для ОО и дано логическое обоснование для такого сопоставления, показывающее, что каждое функциональное требование безопасности для ОО сопоставлено, по крайней мере, с одной целью безопасности для ОО, и что все цели безопасности для ОО надлежащим образом учтены в функциональных требованиях безопасности для ОО. Иначе говоря, если все функциональные требования безопасности для ОО выполнены, то все цели безопасности для ОО достигнуты и имеется доверие к тому, что всем угрозам обеспечено противостояние, все политики безопасности организации осуществлены и все предположения безопасности реализованы, т.е. проблема безопасности решена.

Требования безопасности для среды функционирования ОО здесь не определяются и не обосновываются, поскольку фактически они определены самими целями безопасности для среды функционирования ОО, сформулированными ранее.

6.1 Функциональные требования безопасности

Функциональные требования безопасности, определенные в настоящем ЗБ, основаны на компонентах функциональных требований безопасности, определенных в Профиле защиты ИТ.ОС.А4.ПЗ, и перечислены ниже в Таблице 6.1

6.1.1 Аудит безопасности (FAU)

FAU_ARP.1	**Сигналы нарушения безопасности**
FAU_ARP.1.1	ФБО должны предпринять [информирование администратора **путем генерации и записи информации в журнал регистрации событий безопасности**], [**нет других действий**] при обнаружении возможного нарушения безопасности.
Зависимости:	FAU_SAA.1 Анализ потенциального нарушения.

Таблица 6.1 – Функциональные компоненты, на которых основаны функциональные требования безопасности

Идентификатор компонента требований	**Название компонента требований**
FAU_ARP.1	Сигналы нарушения безопасности
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
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_ETC.2	Экспорт данных пользователя с атрибутами безопасности
FDP_IFC.2	Полное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FDP_RIP.2	Полная защита остаточной информации
FDP_CRC_EXT.1	Восстановление информации
FDP_DDM_EXT.1	Уничтожение (стирание) 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_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.5	Сочетание механизмов аутентификации
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.1	Выбор момента идентификации
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1	Связывание пользователь-субъект
FIA_OID_EXT.1	Идентификация объектов доступа
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными функций безопасности
FMT_MTD.2	Управление ограничениями данных ФБО
FMT_SAE.1	Ограниченная по времени авторизация
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
FMT_UST_EXT.1	Поддержка наборов базовых конфигураций
FPT_FLS.1	Сбой с сохранением безопасного состояния

Идентификатор компонента требований	Название компонента требований
FPT_ITC.1	Конфиденциальность экспортируемых данных функциональных возможностей безопасности объекта оценки при передаче
FPT_RCV.1	Ручное восстановление
FPT_STM.1	Надежные метки времени
FPT_TST.1	Тестирование функциональных возможностей безопасности
FPT_ACF_EXT.1	Управление доступом к компонентам операционной системы
FPT_APW_EXT.1	Защита хранимой аутентификационной информации
FPT_BOP_EXT.1	Защита от переполнения буфера
FPT_MTR_EXT.1	Монитор обращений
FRU_FLT.1	Пониженная отказоустойчивость
FRU_PRS.1	Ограниченный приоритет обслуживания
FRU_RSA.1	Максимальные квоты
FTA_MCS.2	Ограничение на параллельные сеансы по атрибутам пользователя
FTA_SSL.1	Блокирование сеанса, инициированное ФБО
FTA_SSL.2	Блокирование, инициированное пользователем
FTA_SSL.3	Завершение сеанса, инициированное функциональными возможностями безопасности
FTA_TSE.1	Открытие сеанса с объектом оценки
FPO_DFS_EXT.1	Изоляция процессов
FPO_OBF_EXT.1	Блокирование файлов процессами
FPO_RIP_EXT.1	Выделение случайных областей оперативной памяти

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 в столбце «Событие» Таблицы 6.2, а также [**нет других событий**].

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 Таблицу 6.2, [**нет другой информации**].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 6.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_GEN.1	Запись аудита для событий, связанных с истечением установленного администратором срока действия пароля	Идентификатор пользователя ОС
FAU_GEN.1	Запись аудита для событий, связанных с истечением установленного администратором срока действия идентификатора пользователя ОС (учетной записи)	Идентификатор пользователя ОС (учетной записи)
FIA_AFL.1	Блокирование учетной записи в результате превышения максимального числа неуспешных попыток входа в систему	
FMT_MOF.1	Все модификации политики аудита	
FMT_MSA.1	Все модификации значений атрибутов безопасности, используемых для смены начальной аутентификационной информации пользователя ОС после однократного использования	Смена начальной аутентификационной информации пользователя ОС
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)	
FDP_CRC_EXT.1	Применение механизма восстановления информации	
FDP_DDM_EXT.1	Изменение настроек механизмов уничтожения (стирания) данных	
FPO_DFS_EXT.1	Сбои в работе механизма изоляции процессов	
FPT_SDI_EXT.1	Попытки установки внешних модулей уровня ядра, не проверенных разработчиком (производителем), или внешних модулей уровня ядра с нарушенной целостностью	
FAU_STG.3	**Превышение порога заполнения**	

Компонент	Событие	Детализация
	журнала аудита	
FAU_STG.4	**Исчерпание места в журнале аудита или ошибка при записи информации в журнал аудита**	
FIA_SOS.1	**Отклонение верифицированного секрета**	
FMT_MSA.3	**Изменение настроек по умолчанию и начальных значений атрибутов безопасности**	
FMT_SMR.1	**Создание и удаление ролей, назначение ролям прав и пользователей, удаление из ролей прав и пользователей, использование ролей и прав ролей**	
FPT_STM.1	**Изменения значения времени**	
FRU_RSA.1	**Невыполнение операции распределения ресурсов из-за достижения предела ресурса**	
FTA_SSL.1	**Блокирование сеансов, инициированное ФБО, попытки разблокирования**	
FTA_SSL.2	**Блокирование сеансов, инициированное пользователем, попытки разблокирования**	
FTA_TSE.1	**Попытки установления сеанса пользователя**	
FDP_RSP_EXT.2.1	**Попытки запуска компонентов программного обеспечения, произведенных в нарушение установленных правил запуска компонентов программного обеспечения**	
FDP_RSP_EXT.2.2	**Попытки запуска компонентов программного обеспечения, целостность которых была нарушена**	

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [роли администраторов в соответствии с FMT_SMR.1] возможность читать [**всю информацию аудита в соответствии с FAU_GEN.1]** 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_SAR.2 Ограниченный просмотр аудита

FAU_SAR.2.1 ФБО должны запретить доступ всем субъектам доступа к чтению записей аудита, за исключением субъектов доступа, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 Просмотр аудита

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны предоставить возможность выполнения поиска, [***сортировки, упорядочения, нет***] данных аудита, основанного на [**логических отношениях элементов информации аудита, определенной в соответствии с FAU_GEN.1**].

Зависимости: FAU_SAR.1 Просмотр 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, [***идентификатор пользователя ОС, тип события***];
б) [**принадлежность пользователя к указанной роли, результат события (успех/отказ)**].

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 [***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 [**информирование администратора путем генерации и записи информации в журнал регистрации событий безопасности**] если журнал регистрации событий безопасности ОС превышает [**определенную администратором величину**

пространства памяти для журнала регистрации событий безопасности ОС].

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита.

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны [***предотвращать события, подвергающиеся аудиту, исключая предпринимаемые уполномоченным привилегированным субъектом доступа***], обеспечивать возможность передавать данные аудита для внешнего хранения и [**выполнять следующие действия:**
а) остановка всех процессов, способных к генерации записей аудита;
б) переключение в однопользовательский режим;
в) остановка системы],
при переполнении журнала регистрации событий безопасности ОС.

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита.

6.1.2 Защита данных пользователя (FDP)

FDP_ACC.1(1) Ограниченное управление доступом

FDP_ACC.1.1(1) ФБО должны осуществлять [политику дискреционного управления доступом] для [**действующих от имени пользователей субъектов доступа (процессов), объектов доступа (файлов, каталогов, томов, устройств, реестра) и всех операций субъектов над объектами, на которые распространяется дискреционное управление доступом**].

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

FDP_ACC.1(2) Ограниченное управление доступом

FDP_ACC.1.1(2) ФБО должны осуществлять [политику ролевого управления доступом] для [**действующих от имени пользователей субъектов доступа (процессов), объектов доступа (файлов, каталогов, томов, устройств, реестра) и всех операций субъектов над объектами, на которые распространяется ролевое управление доступом**]**.**

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

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 [**атрибутах безопасности субъектов (идентификаторах пользователей и групп) и атрибутах безопасности объектов (списках контроля доступа, битах разрешений, идентификаторах пользователей владельцев и групп владельцев объекта).**

FDP_ACF.1.2(1) ФБО должны осуществлять следующие правила определения того, разрешена ли операция управляемого субъекта доступа на управляемом объекте доступа: [**Субъект должен иметь разрешение на поиск каждого элемента пути к объекту и на требуемый доступ к нему. Субъект получает конкретный тип доступа к объекту**
а) на основании списка контроля доступа, если выполняется одно из следующих условий:
- запрашиваемый тип доступа разрешен согласно записям ACL_USER_OBJ или ACL_OTHER списка контроля доступа для этого объекта; или
- запрашиваемый тип доступа разрешен согласно записям ACL_USER, ACL_GROUP_OBJ или ACL_GROUP списка контроля доступа для этого объекта и такое право дается также записью ACL_MASK при ее наличии; или
- запрашиваемый тип доступа разрешен согласно записи ACL_GROUP_OBJ и запись ACL_ MASK отсутствует в списке контроля доступа для этого объекта;
б) на основании битов разрешения доступа, если выполняется одно из следующих условий:
- субъект имеет идентификатор, совпадающий с идентификатором владельца данного объекта и для владельца запрашиваемый доступ разрешен битами разрешений доступа; или
- предыдущее условие не выполняется, но субъект имеет идентификатор группы, совпадающий с идентификатором группы владельца данного объекта и для этого владельца запрашиваемый доступ разрешен битами разрешений доступа; или
- запрашиваемый доступ разрешен битами разрешений доступа для «всех остальных» субъектов, для которых не выполняются два предыдущих условия;

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: [
а) к объектам файловой системы, смонтированным только на чтение, доступ на запись всегда запрещен, исключая специальные файлы устройств;
б) к объекту файловой системы, отмеченному как неизменяемый, доступ на запись всегда запрещен].

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

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 [**атрибутах безопасности субъектов (идентификаторах и разрешенных ролях) и атрибутах безопасности объектов (идентификаторах и разрешенных правах доступа для Различных ролей].**

FDP_ACF.1.2(2) ФБО должны осуществлять следующие правила определения того, разрешена ли операция управляемого субъекта доступа на управляемом объекте: [**субъекту разрешается выполнение операции на объекте, если субъект может применять роль, набор прав доступа которой включает данную операцию на данном объекте**].

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: [**пользователь, связанный с субъектом, не обладает ролью, которая разрешает операцию доступа к объекту**].

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

FDP_ETC.2 Экспорт данных пользователя с атрибутами безопасности

FDP_ETC.2.1 ФБО должны осуществлять [***ролевую политику управления,*** [**нет иной политики управления**]] при осуществлении резервного копирования объектов доступа [**являющихся объектами файловой системы, представляющими собой пользовательские данные].**

FDP_ETC.2.2 ФБО должны экспортировать данные пользователя с атрибутами безопасности, ассоциированными с данными пользователя.

FDP_ETC.2.3 ФБО должны обеспечить, чтобы при экспорте за пределы экземпляра ОС атрибуты безопасности однозначно ассоциировались с экспортируемыми данными пользователя.

FDP_ETC.2.4 ФБО должны осуществлять следующие дополнительные правила при экспорте данных пользователя из экземпляра ОС: [**нет дополнительных правил**].

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или FDP_IFC.1 Ограниченное управление информационными потоками].

FDP_IFC.2 Полное управление информационными потоками

FDP_IFC.2.1 ФБО должны осуществлять [фильтрацию сетевого потока] для [отправители информации, получатели информации, сетевой трафик] и всех операций перемещения контролируемой ОС информации сетевого трафика к узлам информационной системы и от них, на которые распространяется фильтрация сетевого потока.

FDP_IFC.2.2 ФБО должны обеспечить распространение фильтрации сетевого трафика на все операции перемещения информации от ОС к узлам информационной системы и от них.

Зависимости: FDP_IFF.1 Простые атрибуты безопасности.

FDP_IFF.1 Простые атрибуты безопасности

FDP_IFF.1.1 ФБО должны осуществлять [фильтрацию сетевого потока], основанную на следующих типах атрибутов безопасности субъектов: [

Таблицы 6.3, 6.4

Субъекты	Атрибуты
отправитель	сетевой адрес узла отправителя, [**нет дополнительных атрибутов]**
получатель	сетевой адрес узла получателя, [**нет дополнительных атрибутов**]
[**нет]**	[**нет**]

и информации:

Информация	Атрибуты
сетевой трафик	сетевой протокол, который используется для взаимодействия; транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии); разрешенные/запрещенные протоколы прикладного уровня; [**нет дополнительных атрибутов]**

].

FDP_IFF.1.2 ФБО должны разрешать сетевой поток между управляемым субъектом и управляемой информацией посредством управляемой операции, если выполняются следующие правила: [**выполняются все заданные администратором на основе атрибутов безопасности субъектов и информации наборы цепочек правил проверки сетевых пакетов с директивами, определяющими действия с пакетами, удовлетворяющими условиям правил проверки**].

FDP_IFF.1.3 ФБО должны осуществлять [**дополнительные правила фильтрации сетевых потоков, определяемые заданными администратором цепочками правил трансляции сетевых адресов**].

FDP_IFF.1.4 ФБО должны явно разрешать сетевой поток, основываясь на следующих правилах: [**нет правил**].

FDP_IFF.1.5 ФБО должны явно запрещать сетевой поток, основываясь на следующих правилах: [**должны отклоняться запросы с неправильной адресацией, с некорректной протокольной информацией, с недопустимыми значениями атрибутов безопасности**].

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

FDP_RIP.2 Полная защита остаточной информации

FDP_RIP.2.1 Функциональные возможности безопасности операционной системы должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при [***распределении ресурса, освобождении ресурса***] для всех объектов.

Зависимости: отсутствуют.

FDP_CRC_EXT.1 Восстановление информации

FDP_CRC_EXT.1.1 Функциональные возможности безопасности операционной системы должны обеспечивать восстановление объектов операционных систем из резервных копий, созданных с использованием операционной системы.

FDP_CRC_EXT.1.2 Функциональные возможности безопасности операционной системы должны использовать атрибуты безопасности, ассоциированные с восстанавливаемыми объектами операционной системы.

Зависимости: отсутствуют.

FDP_DDM_EXT.1 Уничтожение (стирание) информациинные

FDP_DDM_EXT.1.1 Функциональные возможности безопасности операционной системы должны обеспечивать

возможность реализации следующих методов уничтожения (стирания) информации [
а) удаление объектов файловой системы путем исключения их из внутренних структур файловой системы;
б) перезапись уничтожаемых (стираемых) объектов файловой системы случайной битовой последовательностью;
в) многократная перезапись уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями;
[**нет других методов**]].

FDP_DDM_EXT.1.2 Функциональные возможности безопасности Операционной системы должны обеспечивать уничтожение (стирание) [**файлов, каталогов, записей реестра,** [**нет других 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 уполномоченными субъектами [**уполномоченные идентифицированные роли в соответствии с FMT_SMR.1**].
Зависимости: отсутствуют.

FDP_RSP_EXT.1 Правила 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 ОС; разрешенных для запуска в процессе функционирования ОС; запрещенных для запуска в процессе функционирования ОС***].
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, выполнять [***оповещение субъекта доступа, выполняющего запуск, и уполномоченных привилегированных субъектов; блокирование попытки запуска;*** **[нет иных действий**]].

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 [***оповещения субъекта доступа, выполняющего запуск, и уполномоченных привилегированных субъектов; блокирование попытки запуска*****; [нет иных действий]].**

Зависимости: FAU_GEN.1 Генерация данных аудита.

6.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [***устанавливаемое администратором положительное целое число*** неуспешных попыток аутентификации***,*** относящихся к **[последовательным попыткам неуспешной аутентификации**].

FIA_AFL.1.2 При достижении или превышении установленного в FIA_AFL.1.1 числа неуспешных попыток аутентификации ФБО должны выполнить [

а) для всех учетных записей администраторов блокировать учетную запись на установленный уполномоченным администратором период, такой, чтобы они не имели возможности предпринять более чем 10 попыток аутентификации за минуту;

б) для всех других учетных записей блокировать учетную запись пользователя до её разблокирования уполномоченным администратором;

в) для всех заблокированных учетных записей реакция на представленные пользователю попытки аутентификации, не будет связана с результатами этих попыток].

Зависимости: FIA_UAU.1 Выбор момента аутентификации.

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя **ОС**

следующий список атрибутов безопасности: [
а) идентификатор пользователя;
б) срок действия учетной записи пользователя;
в) текущее состояние учетной записи пользователя (заблокирована/разблокирована);
г) членство пользователя в группах;
д) пароль пользователя и ограничения, связанные с использованием пароля (срок действия пароля, метрика качества пароля, сведения о ранее использованных паролях и возможностях их повторного использования);
е) ключи для SSH-аутентификации;
ж) список прав для осуществления дискреционного доступа;
з) список ролей для осуществления ролевого доступа].

Зависимости: отсутствуют.

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 ФБО должны предоставить механизм для верификации того, что аутентификационная информация отвечает **[метрике качества, установленной администратором с учетом необходимости обеспечения вероятности того, что аутентификационная информация в течение времени своего существования станет известной нарушителю, меньше, чем 2^-20].**

Зависимости: отсутствуют.

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_UAU.5 Сочетание механизмов аутентификации

FIA_UAU.5.1 ФБО должны предоставлять [
а) механизм парольной аутентификации;
б) механизм SSH-аутентификации;
в) сочетание вышеуказанных механизмов парольной аутентификации и SSH-аутентификации]
для поддержки аутентификации пользователя ОС.

FIA_UAU.5.2 ФБО должны аутентифицировать представленный идентификатор пользователя **ОС** согласно правилам: [
а) если использование аутентификации SSH в сочетании с парольной аутентификацией предусмотрено, то

аутентификация SSH всегда проводится перед парольной аутентификацией;
б) если использование аутентификации SSH в сочетании с парольной аутентификацией предусмотрено и аутентификация SSH прошла успешно, то пользователь считается аутентифицированным и парольная аутентификация не проводится;
в) если использование аутентификации SSH в сочетании с парольной аутентификацией предусмотрено и аутентификация SSH не прошла успешно, то проводится парольная аутентификация и, если она проходит успешно, то пользователь считается аутентифицированным;
г) если парольная аутентификация проводится и не проходит успешно, то пользователь не считается аутентифицированным].

Зависимости: отсутствуют.

FIA_UAU.7 Аутентификация с защищенной обратной связью

FIA_UAU.7.1 ФБО должны предоставлять пользователю ОС только [
а) скрытую информацию обратной связи в виде специальных условных маскировочных знаков, количество которых равняется количеству введенных пользователем символов при предъявлении пароля;
б) скрытую информацию обратной связи в виде протокольных сообщений механизма SSH- аутентификации].
во время выполнения аутентификации.

Зависимости: FIA_UAU.1 Выбор момента аутентификации.

FIA_UID.1 Выбор момента идентификации

FIA_UID.1.1 ФБО должны допускать [
а) **предъявление идентификатора;**
б) предъявление допустимых механизмов аутентификации]
от имени пользователя ОС прежде, чем он идентифицирован.

FIA_UID.1.2 ФБО должны требовать, чтобы каждый пользователь ОС был успешно идентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя ОС.

Зависимости: отсутствуют.

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.

FIA_USB.1 Связывание пользователь-субъект

FIA_USB.1.1 ФБО должны ассоциировать соответствующие атрибуты безопасности пользователя ОС с субъектами доступа, действующими от имени этого пользователя ОС: [
а) идентификатор пользователя, ассоциируемый с событиями аудита;
б) идентификаторы пользователя, используемые при дискреционном управлении доступом;
в) членство пользователя в группах, используемое при дискреционном управлении доступом;
г) роль пользователя, используемая при ролевом управлении доступом].

FIA_USB.1.2 ФБО должны осуществлять следующие правила исходной ассоциации атрибутов безопасности пользователей ОС с субъектами доступа, действующими от имени пользователей ОС: [
а) после успешной идентификации и аутентификации входной идентификатор пользователя, реальный идентификатор пользователя и эффективный идентификатор пользователя должны совпадать со значением идентификатора пользователя, указанным в учетной записи этого пользователя;
б) после успешной идентификации и аутентификации реальный идентификатор группы и эффективный идентификатор группы должны совпадать со значением идентификатора группы, указанным в учетной записи для этой группы;
в) после успешной идентификации и аутентификации роль должна быть одной из допустимых действующих ролей, назначенных пользователю].

FIA_USB.1.3 ФБО должны осуществлять следующие правила управления изменениями атрибутов безопасности пользователей ОС, ассоциированными с субъектами доступа, действующими от имени пользователей ОС: [
а) эффективный идентификатор пользователя может быть изменен выполнением файла программы с установленным атрибутом setuid. В этом случае субъект доступа ассоциируется с эффектиыным идентификатором пользователя владельца программы, а входной нтификатор пользователя и реальный идентификатор пользователя остаются неизменными;
б) эффективный идентификатор пользователя и

реальный идентификатор пользователя могут быть изменены с помощью команды su. В этом случае, если аутентификация прошла успешно, то субъект доступа ассоциируется с измененными эффективным и реальным идентификаторами пользователя, а входной идентификатор пользователя остается неизменным;
в) эффективный идентификатор группы может быть изменен выполнением файла программы с установленным атрибутом setgid. В этом случае субъект доступа ассоциируется с эффектиыным идентификатором группы владельца программы, а реальный идентификатор группы остается неизменным;
г) роль может быть изменена с помощью комаиы newrole. В этом случае, если аутентификация прошла успешно, то субъект доступа ассоциируется с измененной ролью].

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

FIA_OID_EXT.1 Идентификация объектов доступа

FIA_OID_EXT.1.1 Функции безопасности операционной системы должны требовать, чтобы каждый объект доступа операционной системы: [***файл, каталог, том, устройство,*** [нет]] был успешно идентифицирован до разрешения любого действия с ним, осуществляемого при посредничестве других функций безопасности операционных систем.

Зависимости: отсутствуют.

6.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны предоставлять возможность [***определять режим выполнения, отключать, подключать, модифицировать режим выполнения***] функций [
а) идентификации и аутентификации;
б) управления правами доступа;
в) регистрации событий безопасности]
только [администратору].

Зависимости: FMT_SMR.1 Роли безопасности.

FMT_MSA.1(1) Управление атрибутами безопасности

FMT_MSA.1.1(1) ФБО должны осуществлять [***ролевую политику управления,*** **[нет иных политик управления]],** предоставляющую возможность [***изменять значения по умолчанию, запрашивать, модифицировать, удалять***, [**нет других операций**]] атрибуты безопасности [**для осуществления политики дискреционного управления доступом:**

а) определяющие типы доступа;
б) определяющие права доступа]
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.

FMT_MSA.1(2) Управление атрибутами безопасности

FMT_MSA.1.1(2) ФБО должны осуществлять [***ролевую политику управления,*** **[нет иных политик управления]],** предоставляющую возможность [***изменять значения по умолчанию, запрашивать, модифицировать, удалять,*** [**нет других операций**]] атрибуты безопасности [**для осуществления политики ролевого управления доступом:**
а) **определяющие права доступа для ролей;**
б) **определяющие роли для пользователей**]
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.

FMT_MSA.1(3) Управление атрибутами безопасности

FMT_MSA.1.1(3) ФБО должны осуществлять [***ролевую политику управления,*** **[нет иных политик управления]],** предоставляющую возможность [***изменять значения по умолчанию, запрашивать, модифицировать, удалять,*** [**нет других операций**]] атрибуты безопасности [**для осуществления фильтрации сетевых потоков:**
а) определяющие сетевые адреса узлов отправителей и узлов получателей;
б) определяющие порты источника и получателя;
в) определяющие используемые для взаимодействия сетевые протоколы]
только [администратору].

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

FMT_MSA.1(4) Управление атрибутами безопасности

FMT_MSA.1.1(4) ФБО должны осуществлять [***ролевую политику управления,*** **[нет иных политик управления]],** предоставляющую

возможность:
- [присваивать, блокировать, удалять] атрибуты безопасности [идентификаторы пользователей ОС];
- [назначать] атрибуты безопасности [срок действия идентификаторов пользователей ОС];
- [устанавливать] атрибуты безопасности, [связанные со временем доступа пользователей ОС (разрешенное время работы под учетной записью пользователя, неразрешенное время работы под учетной записью пользователя ОС) в ОС] только [администратору];

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

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять осуществлять [***ролевую политику управления,*** **[нет иных политик управления]],** предусматривающую ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ.

FMT_MSA.3.2 ФБО должны позволять [администратору] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта.

Зависимости: FMT_SMR.1 Роли безопасности;
FMT_MSA.1(1) Управление атрибутами безопасности.

FMT_MTD.1 Управление данными ФБО

FMT_MTD.1.1 ФБО должны предоставлять возможность [***выполнения операций, указанных во втором столбце таблицы 6.5, а также*** [**нет других операций**]] следующих данных [***указанных в третьем столбце таблицы 6.5, а также*** [**нет других данных ФБО**]] только [**роли администраторов в соответствии с FMT_SMR.1**].

Таблица 6.5

Компонент	Операция	Данные ФБО
FIA_ATD.1	создание атрибутов пользователя ОС, необходимых для поддержки механизмов защиты информации ОС при принятии решений, связанных с безопасностью	атрибуты пользователя ОС

Компонент	Операция	Данные ФБО
FIA_OID_EXT.1	создание, модификация, удаление	идентификационная информация объектов файловой системы и устройств
FMT_MSA.1	модификация	атрибуты пользователя ОС
FMT_MSA.1	модификация	начальная аутентификационная информация
FMT_MTD.1	модификация	задание срока действия пароля пользователей ОС
FDP_DDM_EXT.1	определение, модификация	параметры уничтожения (стирания) данных

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

FMT_MTD.2 Управление ограничениями данных ФБО

FMT_MTD.2.1 ФБО должны предоставлять возможность определения ограничений для [
а) сроков действия учетных записей;
б) сроков действия паролей и ssh-ключей;
в) числа подряд идущих неуспешных попыток аутентификации;
г) числа параллельных сеансов доступа;
д) длительности времени бездействия пользователей;
е) пространства памяти для журнала регистрации событий безопасности]
только [администратору].

FMT_MTD.2.2 ФБО должны предпринять следующие действия при достижении или превышении данными ФБО установленных выше ограничений: [**блокирование учетных записей, выдача запросов на смену паролей или ssh-ключей**, **генерация соответствующих записей в журнале регистрации событий безопасности**].

Зависимости: FMT_SMR.1 Роли безопасности;
FMT_MTD.1 Управление данными ФБО.

FMT_SAE.1 Ограниченная по времени авторизация

FMT_SAE.1.1 ФБО должны предоставлять возможность назначать срок действия для [список атрибутов безопасности, для которых предусмотрено установление срока действия, приведен в первом столбце таблицы **6.6**] только [ролям, уполномоченным на установление срока действия атрибутов, идентифицированным из числа ролей, определенных в

FMT_SMR.1, и указанным во втором столбце таблицы **6.6**].

FMT_SAE.1.2 Для каждого из этих атрибутов безопасности ФБО должны быть способны к [выполнению действий в соответствии со списком, указанным в третьем столбце таблицы 6.6] по истечении его срока действия.

Таблица 6.6 – Список атрибутов безопасности, для которых предусмотрено установление срока действия

Список атрибутов безопасности, для которых предусмотрено установление срока действия	**Роли, уполномоченные на установление срока действия атрибутов**	**Список действий, предпринимаемых для каждого атрибута безопасности**
идентификатор пользователя	[роли администраторов в соответствии с FMT_SMR.1]	блокирование учетной записи пользователя ОС
аутентификационная информация пользователя	[роли администраторов в соответствии с FMT_SMR.1]	блокирование учетной записи пользователя ОС до смены аутентификационной информации
[**нет иных атрибутов**]	[**нет**]	[**нет**]

Зависимости: FMT_SMR.1 Роли безопасности;
FPT_STM.1 Надежные метки времени.

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], [**нет**].

Зависимости: отсутствуют.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли пользователей ОС: **[**
а) администратор [**нет**];
б) пользователь].

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

Зависимости: FIA_UID.1 Выбор момента идентификации.

FMT_UST_EXT.1 Поддержка наборов базовых конфигураций

FMT_UST_EXT.1.1 Функциональные возможности безопасности операционной системы должны поддерживать возможность применения

наборов базовых конфигураций в зависимости от [***роли средства вычислительной техники, на котором функционирует операционная система; условий эксплуатации***].

Зависимости: отсутствуют.

6.1.5 Защита ФБО

FPT_FLS.1 Сбой с сохранением безопасного состояния

FPT_FLS.1.1 ФБО должны сохранить безопасное состояние при следующих типах сбоев: [
а) в результате которых стали испорчены или недоступны данные о назначенных ролям правах;
б) в результате которых стали испорчены или недоступны данные о уполномоченных на роли пользователях;
в) в результате которых стали испорчены или недоступны подмножества вышеперечисленных данных].

Зависимости: отсутствуют.

FPT_ITC.1 Конфиденциальность экспортируемых данных ФБО при передаче

FPT_ITC.1.1 ФБО должны защитить данные аудита, передаваемые от ФБО к другому доверенному продукту ИТ, от несанкционированного раскрытия при передаче.

Зависимости: отсутствуют.

FPT_RCV.1 Ручное восстановление

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

Зависимости: AGD_OPE.1 Руководство пользователя по эксплуатации.

FPT_STM.1 Надежные метки времени

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

Зависимости: отсутствуют.

FPT_TST.1 Тестирование функциональных возможностей безопасности

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования [***при запуске***, ***периодически в процессе нормального функционирования, по запросу пользователя ОС, при условиях*** [**нет других условий**]] для демонстрации

правильного выполнения [***части ФБО, ФБО***].

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

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

Зависимости: отсутствуют.

FPT_ACF_EXT.1 Управление доступом к компонентам операционной системы

FPT_ACF_EXT.1.1 Функциональные возможности безопасности операционной системы должны запрещать непривилегированным субъектам модифицировать [**компоненты операционной системы**].

FPT_ACF_EXT.1.2 Функциональные возможности безопасности операционной системы должны запрещать непривилегированным субъектам читать [***данные аудита событий безопасности операционной системы,*** [**нет иных типов объектов доступа**]].

Зависимости: отсутствуют.

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 аутентификационной информации в открытом виде.

Зависимости: отсутствуют.

FPT_BOP_EXT.1 Защита от переполнения буфера

FPT_BOP_EXT.1.1 Функциональные возможности безопасности операционной системы должны обеспечивать защиту от выполнения произвольного кода вследствие переполнения буфера путем [***проверка соответствия входных данных размеру выделенной области памяти; запрет выполнения кода, содержащегося в области памяти, выделенной только для данных;*** [**нет иных способов**]].

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, субъектов доступа к информации***,[**нет иных типов**

обращений]].

FPT_MTR_EXT.1.2 Функциональные возможности безопасности операционной системы должны осуществлять проверку правомочности обращений к информации на основе установленных политик [***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.

Зависимости: отсутствуют.

6.1.6. Использование ресурсов

FRU_FLT.1 Пониженная отказоустойчивость

FRU_FLT.1.1 ФБО должны обеспечить [

а**) возможность работы экземпляров операционной системы на нескольких технических средствах в отказоустойчивом режиме, обеспечивающем доступность сервисов и информации;**

б) возможность объединения нескольких технических средств энергонезависимой памяти в RAID-массив, обеспечивающий доступность информации],

когда происходят следующие сбои:

[**выход из строя одного из технических средств**].

Зависимости: FPT_FLS.1 Сбой с сохранением безопасного состояния.

FRU_PRS.1 Ограниченный приоритет обслуживания

FRU_PRS.1.1 ФБО должны установить приоритет каждому субъекту доступа в ФБО.

FRU_PRS.1.2 ФБО должны обеспечить доступ к [**процессорному времени, дисковому пространству внешней памяти, оперативной памяти**] на основе приоритетов, назначенных субъектам доступа.

Зависимости: отсутствуют.

FRU_RSA.1 Максимальные квоты

FRU_RSA.1.1 ФБО должны реализовать максимальные квоты следующих ресурсов: [**процессорное время, дисковое пространство внешней памяти, оперативная память**], которые [***отдельные пользователи ОС, определенные группы пользователей ОС, субъекты доступа***] могут использовать [***одновременно,в течение определенного период а времени***].

Зависимости: отсутствуют.

6.1.7 Доступ к ОО

FTA_MCS.2 Ограничение на параллельные сеансы по атрибутам пользователя

FTA_MCS.2.1 ФБО должны ограничить максимальное число параллельных сеансов, предоставляемых одному и тому же пользователю ОС, согласно **правилу** [**не более установленного администратором максимального числа параллельных сеансов,].**

FTA_MCS.2.2 ФБО должны задать по умолчанию ограничение [**не более установленного администратором количества параллельных**] сеансов пользователя ОС.

Зависимости: FIA_UID.1 Выбор момента идентификации.

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

FTA_SSL.1.1 ФБО должны блокировать интерактивный сеанс после **[истечения установленной администратором длительности времени бездействия пользователя ОС],],** для чего предпринимаются следующие действия:
а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;
б) блокирование любых действий по доступу к данным пользователя (устройствам) отображения, кроме необходимых для разблокирования сеанса.

FTA_SSL.1.2 ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [**повторная аутентификация пользователя ОС**].

Зависимости: FIA_UAU.1 Выбор момента аутентификации.

FTA_SSL.2 Блокирование, инициированное пользователем

FTA_SSL.2.1 ФБО должны допускать инициированное пользователем **ОС** блокирование своего собственного интерактивного сеанса, для чего предпринимаются следующие действия:
а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;
б) блокирование любых действий по доступу к данным пользователя (устройствам) отображения, кроме необходимых для разблокирования сеанса.

FTA_SSL.2.2 ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [**повторная аутентификация пользователя ОС**].

Зависимости: FIA_UAU.1 Выбор момента аутентификации.

FTA_SSL.3 Завершение, инициированное ФБО

FTA_SSL.3.1 ФБО должны завершить интерактивный сеанс после [**истечения установленной администратором длительности**

времени бездействия пользователя ОС].

Зависимости: отсутствуют.

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса, основываясь на [

а) идентификационных данных пользователя;

б) аутентификационных данных пользователя;

в) правах доступа к ОО;

г) установленном администратором времени, когда доступ к ОО запрещен].

Зависимости: отсутствуют**.**

6.1.8 Функциональные возможности безопасности

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, устройства*** [**нет других объектов**]].

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

Зависимости: отсутствуют.

FPO_OBF_EXT.1 Блокирование файлов процессами

FPO_OBF_EXT.1.1 Функциональные возможности безопасности операционной системы должны предоставлять возможность блокирования попытки выполнения следующих операций [***модификация, удаление***] над файлами, если в момент обращения к файлу он используется другим процессом.

Зависимости: отсутствуют.

FPO_RIP_EXT.1 Выделение случайных областей оперативной памяти

FPO_RIP_EXT.1.1 Функциональные возможности безопасности операционной системы должны выделять области оперативной памяти для всех процессов обработки информации [***случайным образом,*** [**нет иных способов выделения памяти**]].

Зависимости: FRU_RSA.1 Максимальные квоты.

6.2. Требования доверия к безопасности

Требования доверия к безопасности ОО совпадают с требованиями к разработке и производству, проведению испытаний и поддержке безопасности средства, соответствующего 4 уровню доверия согласно документу «Требования по безопасности информации, устанавливающе уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденному приказом ФСТЭК России от 2 июня 2020 г. № 76.

6.3 Обоснование требований безопасности

6.3.1 Обоснование функциональных требований безопасности

В данном подразделе представлено отображение функциональных требований безопасности на цели безопасности для ОО с соответствующим обоснованием.

Таблица 6.8 – Отображение функциональных требований безопасности на цели безопасности

	Цель безопасности-1	**Цель безопасности-2**	**Цель безопасности-3**	**Цель безопасности-4**	**Цель безопасности-5**	**Цель безопасности-6**	**Цель безопасности-7**	**Цель безопасности-8**	**Цель безопасности-9**
FAU_ARP.1							**X**		
FAU_GEN.1							**X**		
FAU_SAR.1							**X**		
FAU_SAR.2							**X**		
FAU_SAR.3							**X**		
FAU_SEL.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**							
FDP_ACF.1(2)		**X**							

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9
FDP_ETC.2				X					
FDP_IFC.2						X			
FDP_IFF.1		X				X			
FDP_RIP.2			X						
FDP_CRC_EXT.1				X					
FDP_DDM_EXT.1			X						
FDP_RSI_EXT.1			X						
FDP_RSP_EXT.1			X						
FDP_RSP_EXT.2			X						
FIA_AFL.1	X								
FIA_ATD.1	X								
FIA_SOS.1	X								
FIA_UAU.2	X								
FIA_UAU.5	X								
FIA_UAU.7	X								
FIA_UID.1	X								
FIA_UID.2	X								
FIA_USB.1	X								
FIA_OID_EXT.1	X								
FMT_MOF.1		X							X
FMT_MSA.1(1)		X							X
FMT_MSA.1(2)		X							X
FMT_MSA.1(3)									X
FMT_MSA.1(4)	X								
FMT_MSA.3		X							
FMT_MTD.1	X								X
FMT_MTD.2	X								
FMT_SAE.1	X								X
FMT_SMF.1									X
FMT_SMR.1									X
FMT_UST_EXT.1									X

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9
FPT_FLS.1			X						
FPT_ITC.1							X		
FPT_RCV.1				X					
FPT_STM.1								X	
FPT_TST.1				X					
FPT_ACF_EXT.1				X					
FPT_APW_EXT.1	X								
FPT_BOP_EXT.1			X						
FPT_MTR_EXT.1		X							
FRU_FLT.1					X				
FRU_PRS.1					X				
FRU_RSA.1					X				
FTA_MCS.2			X						
FTA_SSL.1			X						
FTA_SSL.2			X						
FTA_SSL.3			X						
FTA_TSE.1			X						
FPO_DFS_EXT.1			X						
FPO_OBF_EXT.1			X						
FPO_RIP_EXT.1			X						

FAU_ARP.1 Сигналы нарушения безопасности

Выполнение требований данного компонента обеспечивает возможность реагирования при обнаружении событий, указывающих на возможное нарушение безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

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-7** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления администратору всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает возможность просмотра записей аудита только субъектами доступа, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает возможность выборочного просмотра данных аудита (поиск, сортировка, упорядочение данных аудита). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

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

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает возможность защиты хранимых записей аудита от несанкционированного удаления и предотвращения модификации записей аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FAU_STG.3 Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает возможность защиты журнала регистрации событий безопасности ОС от переполнения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает возможность выполнения действий, направленных на предотвращение потери данных аудита при переполнении журнала регистрации событий безопасности ОС. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** 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 согласно назначенной роли 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 целью **Цель безопасности-2** и способствует ее достижению.

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

Выполнение требований данного компонента обеспечивает возможность осуществления управления доступом к объектам доступа ОС на основе ролей. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FDP_CRC_EXT.1 Восстановление информации, содержащейся в ОС

Выполнение требований данного компонента обеспечивает возможность восстановления объектов операционной системы из резервных копий, созданных с использованием операционной системы, и использования ассоциированных с ними атрибутов безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FDP_ETC.2 Экспорт данных пользователя с атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность осуществления резервного копирования объектов файловой системы. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FDP_IFC.2 Полное управление информационными потоками

Выполнение требований данного компонента обеспечивает возможность фильтрации сетевого трафика. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует достижению.

FDP_IFF.1 Простые атрибуты безопасности

Выполнение требований данного компонента обеспечивает возможность задания правил фильтрации сетевого потока. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2**, **Цель безопасности-6** и способствует их достижению.

FDP_DDM_EXT.1 Уничтожение (стирание) информации

Выполнение требований данного компонента обеспечивает возможность удаления объектов файловой системы путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FDP_RIP.2 Полная защита остаточной информации

Выполнение требований данного компонента обеспечивает обеспечение недоступности содержания всей остаточной информации любых ресурсов, контролируемых ОС, при распределении или освобождении ресурса. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FDP_RSI_EXT.1 Управление установкой программного обеспечения

Выполнение требований данного компонента обеспечивает возможность установки программного обеспечения (компонентов программного обеспечения) только уполномоченными привилегированными субъектами доступа. 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 возможность задания правил автоматического запуска компонентов программного обеспечения при загрузке операционной системы. 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_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя ОС список атрибутов безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает ограничение попыток пройти процедуру аутентификации для лиц, не являющихся пользователями ОС. При достижении определенного администратором числа неуспешных попыток аутентификации некоторого лица, ОО предпринимаются действия, направленные на дальнейшее предотвращение попыток доступа со стороны данного лица, ограниченное временным интервалом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает предоставление механизма для верификации соответствия паролей определенным требованиям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** 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 операционной системой. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_UAU.5 Сочетание механизмов аутентификации

Выполнение требований данного компонента обеспечивает возможность выполнения аутентификации с использованием сочетания различных механизмов аутентификации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_UAU.7 Аутентификация с защищенной обратной связью

Выполнение требований данного компонента обеспечивает исключение отображения действительного значения аутентификационной информации при ее вводе пользователем ОС в диалоговом интерфейсе. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_UID.1 Выбор момента идентификации

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

FIA_USB.1 Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает возможность ассоциировать атрибуты безопасности пользователя ОС с запускаемыми от его имени процессами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_OID_EXT.1 Идентификация объектов доступа

Выполнение требований данного компонента обеспечивает идентификацию объекта доступа по запросу механизмов защиты информации ОС, осуществляющих контроль действий над объектом доступа. 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-9** 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 администратору. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2**, **Цель безопасности-9** и способствует их достижению.

FMT_MSA.1(1) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только администратору. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2**, **Цель безопасности-9** и способствует их достижению.

FMT_MSA.1(2) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики ролевого управления доступом только администратору. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2**, **Цель безопасности-9** и способствует их достижению.

FMT_MSA.1(3) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики фильтрации сетевого трафика только администратору. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-9** и способствует ее достижению.

FMT_MSA.1(4) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность возможности управления идентификаторами пользователей ОС. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает возможность определения правил (политики дискреционного управления доступом), которые предпишут значение, которое должен наследовать атрибут безопасности. 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 администратору. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-9** и способствует их достижению.

FMT_MTD.2 Управление ограничениями данных ФБО

Выполнение требований данного компонента обеспечивает возможность задания администратору порогового значения количества неуспешных попыток аутентификации. 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-9** и способствует ее достижению.

FMT_SAE.1 Ограниченная по времени авторизация

Выполнение требований данного компонента обеспечивает возможность администратору устанавливать срок действия определенных атрибутов безопасности. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-9** и способствует их достижению.

FMT_UST_EXT.1 Поддержка наборов базовых конфигураций

Выполнение требований данного компонента обеспечивает возможность поддержки базовых конфигураций в зависимости от роли СВТ, на котором

функционирует ОС и условий эксплуатации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-9** и способствует ее достижению.

FPT_ACF_EXT.1 Управление доступом к компонентам ОС

Выполнение требований данного компонента обеспечивает возможность запрещать пользователям модификацию компонентов ОС и чтение данных аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FPT_ITC.1 Конфиденциальность экспортируемых данных функциональных возможностей безопасности объекта оценки при передаче

Выполнение требований данного компонента обеспечивает возможность защиты данных аудита от несанкционированного раскрытия при их передаче. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FPT_FLS.1 Сбой с сохранением безопасного состояния

Выполнение требований данного компонента обеспечивает сохранение безопасного состояния при сбоях. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FPT_BOP_EXT.1 Защита от переполнения буфера

Выполнение требований данного компонента обеспечивает защиту от выполнения произвольного машинного кода. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** 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 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 хранимой 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.1 Ручное восстановление

Выполнение требований данного компонента обеспечивает возможность возврата ОС к безопасному состоянию, в автоматизированном режиме. 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-8** и способствует ее достижению.

FRU_FLT.1 Пониженная отказоустойчивость

Выполнение требований данного компонента обеспечивает выполнение заданных действий, когда происходят сбои. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FRU_PRS.1 Ограниченный приоритет обслуживания

Выполнение требований данного компонента обеспечивает возможность установления приоритета каждому субъекту и доступ к ресурсам на основе приоритетов. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FRU_RSA.1 Максимальные квоты

Выполнение требований данного компонента обеспечивает возможность реализации максимальных квот ресурсов, которые пользователи могут использовать. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FTA_MCS.2 Ограничение на параллельные сеансы по атрибутам пользователя

Выполнение требований данного компонента обеспечивает ограничение максимального числа параллельных сеансов, предоставляемых одному и тому же пользователю ОС. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

Выполнение требований данного компонента обеспечивает возможность осуществлять средством защиты информации в ОС блокирование сеанса пользователя ОС по истечении заданного периода времени. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FTA_SSL.2 Блокирование, инициированное пользователем

Выполнение требований данного компонента обеспечивает возможность осуществлять блокирование (разблокирование) сеанса. Рассматриваемый

компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FTA_SSL.3 Завершение сеанса, инициированное функциональными возможностями безопасности

Выполнение требований данного компонента обеспечивает возможность осуществлять завершение сеанса, инициированное ФБО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FTA_TSE.1 Открытие сеанса с ОО

Выполнение требований данного компонента обеспечивает возможность отказать в открытии сеанса, основываясь на определенных атрибутах. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FPO_DFS_EXT.1 Изоляция процессов

Выполнение требований данного компонента обеспечивает возможность обеспечения защиты от несогласованностей, возникающих на уровне процессов при параллельной работе с ресурсами средства вычислительной техники и объектами доступа операционной системы. 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 действия над объектами доступа, если в момент обращения объект доступа используется другим процессом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FPO_RIP_EXT.1 Выделение случайных областей оперативной памяти

Выполнение требований данного компонента обеспечивает возможность выделения в ОС для всех процессов обработки информации области оперативной памяти случайным образом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

6.3.2 Обоснование удовлетворения зависимостей функциональных требований безопасности

В таблице 6.9 представлены результаты удовлетворения зависимостей функциональных требований безопасности. Третий столбец таблицы показывает, какие компоненты требований были включены в настоящем ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце. Компоненты требований в третьем столбце таблицы либо совпадают с компонентами во втором столбце, либо иерархичны по отношению к ним. Это свидетельствует, что все зависимости компонентов требований в настоящем ЗБ удовлетворены.

Таблица 6.9 – Зависимости функциональных требований безопасности

Функциональные компоненты	**Зависимости функциональных требований безопасности**	**Удовлетворение зависимостей**
FAU_ARP.1	FAU_SAA.1	Цель для среды функционирования ОО-5
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 FMT_MTD.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.3
FDP_ETC.2	[FDP_ACC.1 или FDP_IFC.1]	FDP_ACC.1
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1

Функциональные компоненты	Зависимости функциональных требований безопасности	Удовлетворение зависимостей
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	FMT_MTD.1 FMT_SMR.1
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	FMT_SMR.1 FPT_STM.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_RCV.1	AGD_OPE.1	AGD_OPE.1
FRU_FLT.1	FPT_FLS.1	FPT_FLS.1
FTA_MCS.2	FIA_UID.1	FIA_UID.2
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2
FTA_SSL.2	FIA_UAU.1	FIA_UAU.2
FPO_RIP_EXT.1	FRU_RSA.1	FRU_RSA.1

Для компонента FAU_ARP.1 невключение по зависимости компонента FAU_SAA.1 компенсировано включением в ПЗ Цели для среды функционирования ОО-5.

6.3.3 Обоснование требований доверия к безопасности объекта оценки

Требования доверия к безопасности ОО настоящего ЗБ совпадают с требованиями к разработке и производству, проведению испытаний и поддержке безопасности средства, соответствующего 4 уровню доверия, согласно документу «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденному приказом ФСТЭК России от 2 июня 2020 г. № 76.

7 Краткая спецификация ОО

В данном разделе представлено краткое описание того, каким образом реализованные в ОО функции безопасности удовлетворяют всем компонентам функциональных требований безопасности (ФТБ), а также описание осуществляемых мер доверия, удовлетворяющих требованиям доверия к безопасности ОО.

7.1 Функции безопасности ОО

Имеющиеся в ОО средства реализуют следующие функции безопасности: идентификация и аутентификация, управление доступом, регистрация событий безопасности, ограничение программной среды, изолция процессов, защита памяти, контроль целостности, обеспечение надежного функционирования, фильтрация сетевого потока.

7.1.1 Идентификация и аутентификация

Доступ к ОО и его ресурсам возможен только для зарегистрированных пользователей, успешно прошедших идентификацию и аутентификацию. Идентификация и аутентификация до любых действий пользователей, а также выбор момента идентификации осуществляются с помощью так называемых модулей PAM и конфигурационных файлов, которые хранятся в /etc/pam.d, с использованием утилит login, unix_chkpwd, su, sudo, ssh, процессов agetty и mingetty. Для предупреждения пользователей при входе в систему о том, что в ней реализованы меры защиты информации и о необходимости соблюдения установленных правил обработки информации, используется файл /etc/issue. С помощью предоставляемых вышеописанными средствами функциональных возможностей обеспечивается выполнение и поддержка следующих компонентов ФТБ: FIA_UAU.2, FIA_UID.1, FIA_UID.2.

Для блокировки учетных записей пользователей, совершивших определенное количество неудачных попыток входа, используется PAM модуль pam_tally2. С помощью предоставляемых им функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FIA_AFL.1.

Информация об учетных записях пользователей и групп хранится в текстовых файлах в каталоге /etc/. В конфигурационных файлах etc/pam.d/system-auth и etc/pam.d/password-auth содержатся важные параметры системы аутентификации. Механизм идентификации и аутентификации выполняет ассоциацию идентификационных данных пользователя с событиями безопасности также в ходе контроля доступа. Для задания и редактирования соответствующей информации используются утилиты useradd, userdel, passwd, ssh-keygen, newrole, newgrp, gpasswd. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка следующих компонентов ФТБ: FIA_ATD.1, FIA_USB.1.

Механизм аутентификации предоставляет пользователю только скрытую информацию обратной связи во время выполнения аутентификации, что достигается за счет использования модулей PAM, конфигурационных файлов, утилит login, unix_chkpwd, su, sudo, процессов agetty, mingetty. Значения паролей хранятся в файле /etc/shadow в защищенном виде. Средства аутентификации так же предоставляют пользователю скрытую информацию обратной связи в виде протокольных сообщений механизма ssh-аутентификации. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FIA_UAU.7.

Парольная аутентификация, ssh-аутентификация и их сочетание регулируются механизмами ssh. С помощью предоставляемых ими функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FIA_UAU.5.

При создании каждого файла в дескриптор записываются имя владельца файла и группы, которая имеет права на этот файл. Тип файла и права доступа к файлу, в том числе символ, идентифицирующий тип файла, определяются в соответствии с реализованными правилами политики безопасности управления доступом, средствами управления доступом, обеспечивающими выполнение и поддержку компонента ФТБ: FIA_OID_EXT.1.

При помощи модулей PAM в системе настраивается механизм верификации того, что аутентификационная информация отвечает метрике качества, что обеспечивает выполнение и поддержку компонента ФТБ: FIA_SOS.1.

Механизмы идентификации и аутентификации предотвращают хранение и чтение аутентификационной информации в открытом виде благодаря настроенным правам доступа, которые определяются в соответствии с реализованными правилами политики безопасности управления доступом, чем обеспечивается выполнение и поддержка компонента ФТБ: FPT_APW_EXT.1.

Таким образом, реализованные в ОО функциональные средства идентификации и аутентификации обеспечивают удовлетворение следующей совокупности ФТБ: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.1, FIA_UID.2, FIA_USB.1, FIA_OID_EXT.1, FPT_APW_EXT.1.

7.1.2 Управление доступом

Средства ОО, реализующие механизмы DAC и RBAC осуществляют управление доступом для субъектов и объектов, основываясь на их атрибутах безопасности и операциях доступа к ним, а так же осуществляют управление режимами выполнения функций идентификации и аутентификации, управления правами доступа и регистрации событий безопасности. С помощью совокупности средств DAC и RBAC для роли администратора предоставляется возможность управления данными ФБО (атрибутами пользователей, идентификационной информацией объектов ФС и устройств, начальной аутентификационной информацией, сроком действия пароля пользователей, параметрами уничтожения данных) и режимами выполнения ФБО. При этом

DAC использует биты разрешений и списки контроля доступа, а так же осуществляет управление доступом к идентификационной информации пользователей и групп с помощью утилит useradd, usermod, groupadd и groupmod. Для изменения и просмотра прав доступа к файлам и каталогам используются утилиты chmod, chattr, ls и lsattr, а для определения списков контроля доступа - утилиты getfacl и setfacl. RBAC основан на использовании системы принудительного контроля доступа SELinux, для управления которой используется утилита semanage, режим функционирования регулируется с помощью утилит getenforce и setenforce, а состояние определяется утилитой sestatus. С помощью утилит newrole и semanage задаются и ассоциируются роли и контекст безопасности пользователя, а с помощью утилиты id они определяются, с помощью утилиты ps определяется контекст безопасности процесса, с помощью утилиты chcon задается SELinux тип безопасности объектов доступа, а утилитой ls он определяется. С помощью предоставляемых вышеописанными средствами функциональных возможностей обеспечивается выполнение и поддержка следующих компонентов ФТБ: FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1.

С помощью средств DAC и RBAC администратор и владелец файла могут управлять атрибутами безопасности для осуществления политик безопасности дискреционного и ролевого управлений доступа. При этом DAC использует биты разрешений и списки контроля доступа, а так же утилиту chown для выбора владельца объекта доступа и утилиты, описанные выше: chmod, chattr, ls, lsattr, getfacl, setfacl. RBAC реализуется с помощью SELinux и использует утилиты seinfo и sesearch для определения роли пользователя и списка доменов, к которым имеет доступ роль, утилиту audit2allow для генерации разрешающих правил доступа SELinux, утилиту semodule для управления пакетами модулей политики SELinux, а так же утилиты, описанные выше: sestatus, newrole, semanage, id, ps, chcon. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка следующих компонентов ФТБ: FDP_ACC.1, FDP_ACF.1, FMT_MSA.1.

С помощью средств RBAC администратор регулирует доступ к определению ограничительных значений по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ, и определению альтернативных начальных значений для отмены значений по умолчанию при создании объекта с помощью SELinux и утилит, описанных выше: chmod, chown, newrole, semanage, id, ps, ls, chcon. Так же в файле /etc/sudoers и в файлах директории /etc/sudoers.d/ может быть описан доступ к Selinux-доменам процессов с заданной ролью для пользователей. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FMT_MSA.3.

Для установки сроков действия идентификатора пользователя администратором используются утилиты usermod и chage, а для последующей блокировки учетной записи и пароля до смены аутентификационной информации - утилиты crontab, usermod и passwd. С помощью предоставляемых

этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FMT_SAE.1.

Для определения ограничений по срокам действия учетных записей и паролей, их последующей блокировки до смены аутентификационной информации администратором используются утилиты crontab, usermod, chage и passwd. Для ограничения числа подряд идущих неуспешных попыток аутентификации, числа параллельных сеансов доступа, длительности времени бездействия пользователей, пространства памяти для журнала регистрации событий безопасности администратором используются правила управления доступом, настраиваемые с помощью битов разрешений, списков контроля доступа, SELinux и утилит, описанных выше: chmod, seinfo, sesearch, sestatus, newrole, semanage, id, ps, ls, chcon. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FMT_MTD.2.

Для определении роли и ассоциации с ней пользователя RBAC использует SELinux и утилиты newrole и semanage. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FMT_SMR.1.

Ограничения возможностей обычных пользователей по записи в системные каталоги и модификации системных компонент, нарушения в которых может привести ОО в нерабочее состояние, а также по чтению записей регистрации событий безопасности реализуется с помощью битов разрешений, списков контроля доступа и средств системы SELinux. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_ACF_EXT.1.

Для получения информации о том, какие файлы и какая информация используются теми или иными процессами во время функционирования ОО и к какому владельцу они имеют отношение, предназначена утилита lsof. Для получения списка работающих в системе процессов используется утилита top, которая выводит информацию о выполняемых процессах и используемых ими процессорных ресурсах. Правомочность обращений к информации на основе установленных политик управления доступом и информационными потоками, а так же отклонение или удовлетворение данных обращений реализуется с помощью битов разрешений, списков контроля доступа и средств системы SELinux. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_MTR_EXT.1.

Для каждого субъекта в структуре task_struct устанавливается приоритет использования ресурсов и обеспечивается доступ к процессорному времени, дисковому пространству внешней памяти, оперативной памяти на основе данного приоритета. Переназначить приоритет можно утилитой renice. Данные параметры отображают утилиты top и nice. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FRU_PRS.1.

Для реализации максимальных квот процессорного времени, дискового пространства внешней памяти или оперативной памяти, которые отдельные пользователи, или группы пользователей, или субъекты доступа могут использовать одновременно или в течение определенного периода времени используются утилиты quota, edquota, а так же repquota, которая создает полную информацию об использовании дискового пространства и квотах. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FRU_RSA.1.

Для задания максимального числа параллельных сеансов, предоставленных одному и тому же пользователю, администратору необходимо отредактировать файлы /etc/security/limits.conf и /etc/pam.d/system-auth. С помощью предоставляемых этими конфигурационными файлами возможностей обеспечивается выполнение и поддержка компонента ФТБ: FTA_MCS.2.

Определить значение времени бездействия, после которого выполняется блокирование сеанса, очистка и перезапись устройств отображения, можно с помощью утилиты gsettings. Для разблокирования сеанса используются настройки модулей PAM. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка следующих компонентов ФТБ: FTA_SSL.1, FTA_SSL.2.

Завершение сеанса после определенного периода бездействия осуществляется путем редактирования файла /etc/profile. С помощью предоставляемых этим конфигурационным файлом возможностей обеспечивается выполнение и поддержка компонента ФТБ: FTA_SSL.3.

Возможность открытия сеансов на основании идентификационных и аутентификационных данных, правах доступа и установленном администратором времени, когда доступ не запрещен, основана на настройках модулей PAM. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FTA_TSE.1.

Блокирование файлов выполняющимися процессами осуществляется путем использования системного вызова fcntl с запросом режима блокировки F_GETLK. С помощью предоставляемых этим средством функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPO_OBF_EXT.1.

Таким образом, реализованные в ОО функциональные средства управления доступом обеспечивают удовлетворение следующей совокупности ФТБ: FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2 FMT_SAE.1, FMT_SMF.1, FMT_SMR.1, FPT_ACF_EXT.1, FPT_MTR_EXT.1, FRU_PRS.1, FRU_RSA.1, FTA_MCS.2, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3, FTA_TSE.1, FPO_OBF_EXT.1.

7.1.3 Регистрация событий безопасности

Для осуществления контроля за состоянием безопасности в ОО предусмотрены средства регистрации событий безопасности (аудита), режим

функционирования которых может настраиваться и определять: события безопасности, подлежащие регистрации, состав и содержание информации о регистрируемых событиях, возможности выборочного просмотра результатов регистрации событий безопасности, порядок реагирования на сбои при регистрации событий безопасности.

Каждый связанный с безопасностью системный вызов, выполняемый процессом, оценивается в ядре. Все связанные с безопасностью системные вызовы процесса прерываются при входе или выходе из кода системного вызова. Механизм реализации прерывания системных вызовов реализуется функциями audit_syscall_exit() и audit_syscall_entry(). Для прерванной функции оценивается предполагаемое действие, а контекст аудита применяется для соответствующей записи аудита. После чего запись аудита помещается в netlink; а уже оттуда через демон auditd под управленем библиотеки libaudit передается в журнал аудита. Настройка auditd осуществляется в файле auditd.conf. Для запуска и остановки демона аудита используется скрипт init (/etc/init.d/auditd). Для создания и редактирования правил аудита audit.rules используется программа auditctl. Изменения полномочий, а также получение доступа и модификация атрибутов безопасности объекта с помощью chown, chmod, setxattr и removexattr, контролируются с помощью функции audit_inode(). Способы перехвата напрямую обновляют inode информацию для контекста аудита. Генерация записи аудита для ФС связана с подсистемой inotify, предназначенной для обеспечения необходимого функционала отслеживания изменений ФС. С помощью предоставляемых вышеописанными средствами функциональных возможностей обеспечивается выполнение и поддержка следующих компонентов ФТБ: FAU_GEN.1, FAU_ARP.1, FAU_STG.3.

Настройка поведения службы аудита, которая при исчерпании дискового пространства или при возникновении ошибки ввода-вывода будет переключать машину в однопользовательский режим, останавливать процессы, способные к генерации записей аудита, и саму систему, осуществляется с помощью демона auditd и его конфигурации в файле auditd.conf. С помощью предоставляемых этим средством функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FAU_STG.4.

Возможность чтения всей информации аудита предоставляется только для роли администратора и субъектам, которым явно предоставлен доступ, на основании правил политики контроля доступа. Записи аудита предоставляются в виде, позволяющем администратору воспринимать содержащуюся в них информацию, благодаря утилитам aureport, ausearch и autrace. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FAU_SAR.1.

Доступ к чтению записей аудита предоставляется только субъектам, которым явно предоставлен доступ, на основании правил политики контроля доступа. Модуль pam_loginuid.so позволяет реализовать ассоциацию uid входа в систему для установки пользовательского login_uid в контексте аудита, используя функцию ядра audit_set_loginuid(), после чего login_uid сохраняется неизменным для всех операций пользователя на протяжении всего сеанса. С

помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FAU_SAR.2.

Утилиты ausearch и aureport предназначены для поиска, сортировки, упорядочения и фильтрации данных аудита. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FAU_SAR.3.

Выбор совокупности событий, подвергающихся аудиту, из совокупности событий, потенциально подвергаемых аудиту, базируясь на заданных атрибутах, осуществляется с помощью заданий правил регистрации событий утилитой auditctl и корректировки правил аудита в файле audit.rules. Поиск записей аудита осществляется утилитой ausearch. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FAU_SEL.1.

Защита записей аудита в журнале регистрации событий безопасности от несанкционированного удаления и модификации осуществляется на основании правил политики контроля доступа. Попытки модификации журналов аудита регистрируются благодаря демону auditd и его конфигурации в файле auditd.conf. Администратор может получать данные сведения, просматривая отчеты с помощью утилиты aureport. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FAU_STG.1.

Для отправки логов подсистемы аудита в централизованное хранилище используется плагин audisp-remote, который входит в входит в пакет audispd-plugins. Конфигурационные файлы всех плагинов хранятся в директории /etc/audisp/plugins.d. Данные аудита могут передаваться для внешнего хранения по протоколу прикладного уровня SFTP. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_ITC.1.

Таким образом, реализованные в ОО функциональные средства регистрации событий безопасности обеспечивают удовлетворение следующей совокупности ФТБ: FAU_ARP.1, FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG.3, FAU_STG.4, FPT_ITC.1.

7.1.4 Ограничение программной среды

Возможность выбора и установки базовых конфигураций и дополнений к ним в зависимости от роли средства вычислительной техники, на котором функционирует ОС, и условий эксплуатации реализована в системе с помощью программы Anaconda. С помощью предоставляемых этим средством функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FMT_UST_EXT.1.

Установка ПО в системе осуществляется уполномоченными субъектами с помощью утилит yum и rpm, ограничение на использование которых накладывают ИФБО управления доступом. С помощью предоставляемых этими

утилитами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FDP_RSI_EXT.1.

Управление загрузкой компонентов ПО для автоматического запуска во время загрузки ОС осуществляет служба systemd, управляемая утилитой systemctl. Разрешение и запрет для запуска компонентов во время функционирования системы осуществляется под управлением средств управления доступом. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FDP_RSP_EXT.1.

Контроль целостности компонентов ПО осуществляется с помощью утилиты md5, автоматизация данного процесса осуществляется с помощью демона cron и утилиты crontab. При нарушении установленных правил запуска компонентов ПО пользователь получает сообщение о нарушении доступа и блокируется попытка запуска с помощью средств управления доступом. Фиксация нарушений в журнале безопасности и оповещение администратора осуществляется путем применения средств регистрация событий безопасности. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FDP_RSP_EXT.2.

Защита от переполнения буфера реализована на основании технологии защиты и сегментации исполняемой памяти ExecShield, которая в свою очередь поддерживает технологию No eXecute. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_BOP_EXT.1.

Таким образом, реализованные в ОО функциональные средства ограничения программной среды обеспечивают удовлетворение следующей совокупности ФТБ: FDP_RSI_EXT.1, FDP_RSP_EXT.1, FDP_RSP_EXT.2, FMT_UST_EXT.1, FPT_BOR_EXT.1.

7.1.5 Изоляция процессов

Каждый процесс в ОО выполняется в выделенном ему изолированном адресном пространстве. Параллельная работа с областями памяти, файлами и устройствами на уровне процессов обеспечивается за счет использования механизмов ядра ОС, которые соблюдают разделение адресных пространств различных процессов при помощи использования регионов областей памяти. Вся информация, связанная с адресным пространством процесса, включена в дескриптор памяти mm_struct, на который ссылается поле mm дескриптора процесса task_struct. Помимо этого изоляция параллельных процессов в оперативной памяти осуществляется с помощью приложения Docker, использующего технологию cgroups для распределения ресурсов и ФС union file system, и пространство имен ядра системы, которое использует системные вызовы clone(), setns() и unshare(). С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPO_DFS_EXT.1.

Расположение стека каждого процесса и начало области памяти выбирается случайно. Вся информация, связанная с адресным пространством процесса, включена в дескриптор памяти (mm_struct), на который ссылается поле mm дескриптора процесса task_struct. Дескриптор памяти процесса указывает на местонахождение дескрипторов VMA. В свою очередь VMA представляет собой непрерывный диапазон виртуальных адресов, в котором области никогда не перекрывают друг друга. Каждая область памяти представлена структурой vm_area_struct. ExecShield предоставляет рандомизацию расположения адресного пространства для системного вызова mmap(), позволяющего выполнить отображение файла или устройства на память. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPO_RIP_EXT.1.

Таким образом, реализованные в ОО функциональные средства изоляции процессов обеспечивают удовлетворение следующей совокупности ФТБ: FPO_DFS_EXT.1, FPO_RIP_EXT.1.

7.1.6 Защита памяти

Недоступность любого предыдущего информационного содержания ресурсов при их распределении и освобождении на уровне ядра достигается через управление фреймами страниц с использованием функции get_zeroed_page(), управление областями памяти с помощью алгоритма Buddy System и схемы Slab allocator, а также управление несмежными областями памяти через функцию vmalloc(). С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FDP_RIP.2.

Удаление объектов ФС путем исключения их из внутренних структур ФС, перезапись уничтожаемых (стираемых) объектов ФС случайной битовой последовательностью, многократная перезапись уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями, уничтожение (стирание) файлов и каталогов осуществляется с помощью утилит sdel, sdmem, sswap, sfill, dd, shred и scrub. С помощью предоставляемых этими утилитами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FDP_DDM_EXT.1.

Таким образом, реализованные в ОО функциональные средства защиты памяти обеспечивают удовлетворение следующих ФТБ: FDP_RIP.2, FDP_DDM_EXT.1.

7.1.7 Контроль целостности

Контроль целостности компонентов ПО осуществляется с помощью настроек системного журналирования демона syslogd и файла конфигурации syslog.conf, а также с помощью утилит пакета coreutils. Автоматизация данного процесса осуществляется с помощью демона cron и утилиты crontab. При нарушении установленных правил запуска компонентов ПО пользователь

получает сообщение о нарушении доступа и блокируется попытка запуска с помощью средств управления доступом. Фиксация нарушений в журнале безопасности и оповещение администратора осуществляется средствами регистрации событий безопасности. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FDP_RSP_EXT.2.

Пакет программ самотестирования выполняется при запуске утилитой rbac-self-test-helper и по запросу пользователя утилитой rbac-self-test, использующей в свою очередь систему утилит AIDE. Для настройки запуска в процессе нормального функционирования программы rbac-self-test используются демон cron и утилита crontab. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_TST.1.

Таким образом, реализованные в ОО функциональные средства контроля целостности обеспечивают удовлетворение следующих ФТБ: FDP_RSP_EXT.2, FPT_TST.1.

7.1.8 Обеспечение надежного функционирования

Средства, реализующие данную функцию, обеспечивают возможность возврата ОО при сбоях и отказах к безопасному состоянию в ручном и автоматизированном режиме, а также возможность восстановления объектов ОО из созданных с использованием ОС резервных копий и использования ассоциированных с ними атрибутов безопасности. Резервное копирование и восстановление для обеспечения сохранности данных ФС и пользователя, экспорт данных с атрибутами безопасности, ассоциированных с данными пользователя, выполняется утилитами tar, cpio и rsync, использование которых осуществляется с соблюдением правил управления доступом. Для системного планирования и автозапуска заданий резервного копирования используются утилиты cron и crontab. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка следующих компонентов ФТБ: FDP_ETC.2, FDP_CRC_EXT.1.

Сохранение безопасного состояния при искажении или утрате данных ролевой политики доступа осуществляется за счет средств управления доступом и средств резервного копирования: утилит tar, cpio и rsync. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_FLS.1.

Возможность возврата системы при сбоях и отказах к безопасному состоянию осуществляется с помощью программ Corosync и Pacemaker, управление конфигурацией которых реализуется утилитой pcs. Возможность проверить и устранить ошибки в ФС при переходе в режим аварийной поддержки выполняется с помощью утилиты fsck. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_RCV.1.

Возможность работы экземпляров ОС на нескольких технических средствах в отказоустойчивом режиме, обеспечивающем доступность сервисов и информации, осуществляется с помощью программ Corosync и Pacemaker, управление конфигурацией которых реализуется утилитой pcs. При выходе из строя одного из технических средств, объединенного с другим техническим средством энергонезависимой памяти в RAID-массив, доступность информации обеспечивается утилитой mdadm. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FRU_FLT.1.

Настройка надежных временных меток в системе осуществляется с помощью утилиты hwclock. Определение времени создания, доступа или модификации файла реализуется утилитой stat. Дата и время в системе определяются командой date. С помощью предоставляемых этими средствами функциональных возможностей обеспечивается выполнение и поддержка компонента ФТБ: FPT_STM.1.

Таким образом, реализованные в ОО функциональные средства обеспечения надежного функционирования удовлетворяют следующим ФТБ: FDP_ETC.2, FDP_CRC_EXT.1, FPT_FLS.1, FPT_RCV.1, FPT_STM.1, FRU_FLT.1.

7.1.9 Фильтрация сетевого потока

Фильтрация сетевых потоков для сетевого трафика, отправителя и получателя информации и всех операций перемещения контролируемой ОС информации к узлам информационной системы и от них осуществляется на канальном уровне с помощью механизм фильтрации для мостов ebtables, а на сетевом уровне - с помощью платформы Netfilter, утилитами Firewalld, firewall-cmd, firewall-config, Iptables. Для проверки связи на удаленной машине и настройки конфигурации IPv4 и IPv6 используются команды ping и ping6 соответственно. С помощью реализуемых данными средствами ИФБО так же выполняется фильтрация, заданная администратором на основе атрибутов безопасности субъектов и наборов цепочек правил проверки сетевых пакетов с директивами, определяющими действия с пакетами, удовлетворяющими условиям правил проверки, и цепочками правил трансляции сетевых адресов. Благодаря средствам управления доступом запросы с неправильной адресацией, некорректной протокольной информацией и недопустимыми значениями атрибутов безопасности отклоняются, запрещая сетевой поток.

Таким образом, имеющиеся в ОО функциональные средства фильтрации сетевого потока обеспечивают удовлетворение следующим ФТБ: FDP_IFC.2, FDP_IFF.1.

Ниже в Таблице 7.1 представлено обобщенное сопоставление всех вышеописанных функций безопасности и сформулированных в предыдущем разделе функциональных требований безопасности, демонстрирующее, что с помощью реализованных в ОО функций безопасности обеспечивается выполнение всех функциональных требований безопасности.

Таблица 7.1 – Сопоставление функций безопасности с функциональными требованиями безопасности

	Идентификация и аутентификация	**Управление доступом**	**Регистрация событий безопасности**	**Ограничение программной среды**	**Изоляция процессов**	**Защита памяти**	**Контроль целостности**	**Обеспечение надежного функционирования**	**Фильтрация сетевого потока**
FAU_ARP.1			**X**						
FAU_GEN.1			**X**						
FAU_SAR.1			**X**						
FAU_SAR.2			**X**						
FAU_SAR.3			**X**						
FAU_SEL.1			**X**						
FAU_STG.1			**X**						
FAU_STG.3			**X**						
FAU_STG.4			**X**						
FDP_ACC.1		**X**							
FDP_ACF.1		**X**							
FDP_ETC.2								**X**	
FDP_IFC.2									**X**
FDP_IFF.1									**X**
FDP_RIP.2						**X**			
FDP_CRC_EXT.1								**X**	
FDP_DDM_EXT.1						**X**			
FDP_RSI_EXT.1				**X**					
FDP_RSP_EXT.1				**X**					
FDP_RSP_EXT.2				**X**			**X**		
FIA_AFL.1	**X**								
FIA_ATD.1	**X**								
FIA_SOS.1	**X**								
FIA_UAU.2	**X**								
FIA_UAU.5	**X**								
FIA_UAU.7	**X**								

	Идентификация и аутентификация	Управление доступом	Регистрация событий безопасности	Ограничение программной среды	Изоляция процессов	Защита памяти	Контроль целостности	Обеспечение надежного функционирования	Фильтрация сетевого потока
FIA_UID.1	X								
FIA_UID.2	X								
FIA_USB.1	X								
FIA_OID_EXT.1	X								
FMT_MOF.1		X							
FMT_MSA.1		X							
FMT_MSA.3		X							
FMT_MTD.1		X							
FMT_MTD.2		X							
FMT_SAE.1		X							
FMT_SMF.1		X							
FMT_SMR.1		X							
FMT_UST_EXT.1				X					
FPT_FLS.1								X	
FPT_ITC.1			X						
FPT_RCV.1								X	
FPT_STM.1								X	
FPT_TST.1							X		
FPT_ACF_EXT.1		X							
FPT_APW_EXT.1	X								
FPT_BOP_EXT.1				X					
FPT_MTR_EXT.1		X							
FRU_FLT.1								X	
FRU_PRS.1		X							
FRU_RSA.1		X							
FTA_MCS.2		X							
FTA_SSL.1		X							
FTA_SSL.2		X							

	Идентификация и аутентификация	Управление доступом	Регистрация событий безопасности	Ограничение программной среды	Изоляция процессов	Защита памяти	Контроль целостности	Обеспечение надежного функционирования	Фильтрация сетевого потока
FTA_SSL.3		**X**							
FTA_TSE.1		**X**							
FPO_DFS_EXT.1					**X**				
FPO_OBF_EXT.1		**X**							
FPO_RIP_EXT.1					**X**				

7.2 Меры доверия к безопасности ОО

Для удовлетворения требований доверия к безопасности ОО были предприняты меры, касающиеся разработки и производства, проведения испытаний и поддержки безопасности.

7.2.1 Разработка и производство

При разработке ОС были предприняты следующие меры:

разработана непротиворечивая модель безопасности, отражающая реализуемые политики управления доступом и фильтрации информационных потоков;

спроектирована архитектура безопасности, обеспечивающая защищенность процесса инициализации и невозможность обхода функциональных возможностей, осуществляющих выполнение ФТБ;

разработана функциональная спецификация, описывающая интерфейсы функций безопасности (ИФБО), их назначения и способы использования, связанные с ними режимы функционирования, параметры и действия;

разработан проект на уровне подсистем и модулей, реализующих ИФБО, упомянутые в функциональной спецификации, в котором описано взаимодействие подсистем и модулей между собой, прослеживание их к соответствующим ИФБО, приведен перечень файлов исходных текстов программного обеспечения ОС с указанием значений контрольных сумм и прослеживание их к соответствующим модулям, приведенным в описании проекта;

разработано описание примененных для создания ОС инструментальных средств разработки, содержащее перечень используемых языков программирования, компиляторов, программных библиотек, отдельных инструментальных программных средств, а также описание порядка компиляции и сборки инсталляционного дистрибутива ОС из исходных текстов;

разработан и выполняется план управления конфигурацией ОС, устанавливающий порядок идентификации, учета, контроля и аудита всех элементов и составных частей конфигурации с целью обеспечения ее управляемости;

разработана документация по безопасной разработке, описывающая используемую модель жизненного цикла и содержание всех физических, процедурных, организационных и других мер безопасности, необходимых для защиты конфиденциальности и целостности проекта ОС на всем протяжении его жизненного цикла;

разработано руководство пользователя, содержащее описание принципов безопасной работы, возможных и доступных функций безопасности, включая параметры и режимы функционирования, описание мер безопасности, направленных на достижение имеющих отношение к пользователям целей безопасности, а также руководство администратора, содержащее описание порядка и процедур безопасной приемки, установки, настройки и контроля функционирования ОС в процессе эксплуатации, описание других мер безопасности, предназначенных для достижения имеющих отношение к администрированию целей безопасности.

7.2.2 Проведение испытаний

В ходе проведения испытаний разработан и выполнен план тестирования, включающий сравнение ожидаемых и фактических результатов тестирования функций безопасности, анализ покрытия тестами и анализ глубины тестирования, свидетельствующие о том, что все функции безопасности реализованы в соответствии с проектными спецификациями, и что фактические результаты тестирования соответствуют ожидаемым, а также включающий проведение испытаний по выявлению уязвимостей и недекларированных возможностей и проведение анализа скрытых каналов.

7.2.3 Поддержка безопасности

Поддержка безопасности обеспечивается регламентацией и соблюдением процедур безопасной поставки ОС потребителям, мониторинга обнаруженных недостатков, разработки исправляющих обновлений, анализа влияния обновлений на задание по безопасности и реализованные функции безопасности, информирования пользователей о недостатках и предоставления им исправляющих обновлений с соответствующими инструкциями по установке, информирования об окончании производства и (или) поддержки.