ЦЕНТР БЕЗОПАСНОСТИ ИНФОРМАЦИИ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ОПЕРАЦИОННЫЕ СИСТЕМЫ
КЛИЕНТСКИЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ
ПРОФИЛЬ ЗАЩИТЫ
ОС.КОС.ПЗ

Версия 1.0

2003

ПРЕДИСЛОВИЕ

Настоящий профиль защиты определяет требования безопасности для клиентских операционных систем.

Операционные системы, соответствующие настоящему профилю защиты, могут использоваться в автоматизированных системах, обрабатывающих конфиденциальную информацию.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ ПЗ 5

1.1 Идентификация ПЗ 5
1.2 Аннотация ПЗ 6
1.3 Соглашения 6
1.4 Термины 7
1.5 Организация ПЗ 7

2 ОПИСАНИЕ ОО 9

2.1 Тип продукта ИТ 9
2.2 Основные функциональные возможности ОО 10
2.2.1 Основные функциональные возможности обеспечения функционирования 10
2.2.2 Основные функциональные возможности по предоставлению интерфейсов 13
2.2.3 Основные функциональные возможности обеспечения безопасности 14

3 СРЕДА БЕЗОПАСНОСТИ ОО 17

3.1 Предположения безопасности 17
3.2 Угрозы 18
3.3 Политика безопасности организации 19

4 ЦЕЛИ БЕЗОПАСНОСТИ 21

4.1 Цели безопасности для ОО 21
4.2 Цели безопасности для среды 22

5 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ 23

5.1 Функциональные требования безопасности ОО 23
5.1.1 Аудит безопасности (FAU) 24
5.1.2 Защита данных пользователя (FDP) 28
5.1.3 Идентификация и аутентификация (FIA) 30
5.1.4 Управление безопасностью (FMT) 32
5.1.5 Защита ФБО (FPT) 36
5.1.6 Доступ к ОО (FTA) 37
5.1.7 Доверенный маршрут/канал (FTP) 38
5.2 Требования доверия к безопасности ОО 39
5.2.1 Управление конфигурацией (ACM) 39
5.2.2 Поставка и эксплуатация (ADO) 39
5.2.3 Разработка (ADV) 40
5.2.4 Руководства (AGD) 41
5.2.5 Тестирование (ATE) 43
5.2.6 Оценка уязвимостей (AVA) 43

6 ОБОСНОВАНИЕ 45

6.1 Логическое обоснование целей безопасности 45
6.1.1 Логическое обоснование целей безопасности для ОО 45
6.1.2 Логическое обоснование целей безопасности для среды 47
6.2 Логическое обоснование требований безопасности 49
6.2.1 Логическое обоснование функциональных требований безопасности 49
6.2.2 Логическое обоснование требований доверия 58
6.2.3 Логическое обоснование зависимостей требований 58
6.3 Логическое обоснование требований к стойкости функций безопасности .60

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИТ – информационные технологии
ОДФ – область действия ФБО
ОК – Общие критерии
ОО – объект оценки
ОС – операционная система
ОУД – оценочный уровень доверия к безопасности
ПБО – политика безопасности ОО
ПЗ – профиль защиты
ПО – программное обеспечение
ПФБ – политика функции безопасности
СФБ – стойкость функции безопасности
ФБО – функции безопасности ОО
ФТБ – функциональные требования безопасности

1 Введение ПЗ

Данный раздел содержит информацию общего характера. Подраздел «Идентификация ПЗ» предоставляет маркировку и описательную информацию, которые необходимы, чтобы идентифицировать, каталогизировать ПЗ и ссылаться на него. Подраздел «Аннотация ПЗ» содержит общую характеристику ПЗ, позволяющую определить применимость настоящего ПЗ в конкретной ситуации. В подразделе «Соглашения» дается описание операций конкретизации компонентов требований безопасности ИТ. В подразделе «Термины» представлены определения основных терминов, специфичных для данного ПЗ. В подразделе «Организация ПЗ» дается пояснение организации документа.

1.1 Идентификация ПЗ

Название ПЗ:	Операционные системы. Клиентские операционные системы. Профиль защиты.
Версия ПЗ:	Версия 1.0.
Обозначение:	ОС.КОС.ПЗ.
Идентификация ОО:	Клиентские операционные системы.
Уровень доверия:	ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности).
Идентификация ОК:	ГОСТ Р ИСО/МЭК 15408—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, Гостехкомиссия России, 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002. Руководящий документ. Безопасность информационных

технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.

Ключевые слова: Операционная система, средство защиты информации, дискреционное управление доступом, профиль защиты, ОУД1.

1.2 Аннотация ПЗ

Настоящий ПЗ определяет требования безопасности для клиентских операционных систем (далее – объект оценки).

Объект оценки (ОО) – клиентская многозадачная и многопользовательская операционная система, обеспечивающая контролируемую защиту доступа (обычно именуемую дискреционным управлением доступом) субъектов (то есть, процессов пользователей) к объектам (например, данным или системным ресурсам) и располагающая возможностями по управлению используемыми аппаратными средствами.

Функционирование ОО подчинено определенной политике безопасности ОО, отраженной в функциональных требованиях безопасности ОО.

Функциональные требования безопасности ОО включают все ФТБ, сформулированные в ПЗ "Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999", а также содержат дополнительные по отношению к ним ФТБ, исходя из специфики ОО "Клиентская операционная система".

Операционные системы, соответствующие настоящему ПЗ, могут использоваться в автоматизированных системах, обрабатывающих конфиденциальную информацию.

1.3 Соглашения

Общие критерии допускают выполнение определенных в части 2 ОК операций над функциональными требованиями. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор» и «назначение».

Операция **«уточнение»** используется для добавления к требованию некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей его удовлетворения. Результат операции **«уточнение»** в настоящем ПЗ обозначается **полужирным текстом**.

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

Операция **«назначение»** используется для присвоения конкретного значения ранее неконкретизированному параметру, такому, например, как длина пароля. Операция **«назначение»** обозначается заключением значения параметра в квадратные скобки, [назначенное значение].

Замечания по применению предназначены либо для разъяснения назначения некоторого требования, идентификации вариантов реализации, либо для определения условий выполнения требования. В случае использования, замечания по применению следуют за компонентом требования.

1.4 Термины

Ниже приводятся определения ряда терминов, используемых в настоящем ЗБ.

Идентификатор – уникальный признак уполномоченного субъекта, однозначно его идентифицирующий.

Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора.

Субъект – сущность в пределах ОДФ, которая инициирует выполнение операций.

Объект – сущность в пределах ОДФ, которая содержит или получает информацию, и над которой субъекты выполняют операции.

1.5 Организация ПЗ

Раздел 1 «Введение ПЗ» содержит информацию управления документооборотом и описательную информацию, необходимые для идентификации ПЗ и ОО, к которому он относится.

Раздел 2 «Описание ОО» содержит описание функциональных возможностей, среды функционирования и границ ОО, служащее цели лучшего понимания его требований безопасности и дающее представление о типе продукта.

Раздел 3 «Среда безопасности ОО» содержит описание аспектов среды безопасности ОО. В данном разделе определяется совокупность угроз, имеющих отношение к безопасному функционированию ОО, политика безопасности организации, которой должен следовать ОО, и предположения (обязательные условия) безопасного использования ОО.

В разделе 4 «Цели безопасности» определена совокупность целей безопасности для ОО и среды функционирования ОО.

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 ОК определены, соответственно, функциональные требования безопасности ИТ и требование доверия к безопасности.

В Разделе 6 «Обоснование» демонстрируется, что ПЗ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, а также, что ОО учитывает идентифицированные аспекты среды безопасности ИТ.

2 Описание ОО

2.1 Тип продукта ИТ

Объектом оценки в настоящем ПЗ является клиентская операционная система.

Объект оценки – клиентская многозадачная и многопользовательская операционная система, обеспечивающая контролируемую защиту доступа (обычно именуемую дискреционным управлением доступом) субъектов (то есть, процессов пользователей) к объектам (например, данным или системным ресурсам) и располагающие возможностями по управлению используемыми аппаратными средствами.

Функционированию клиентских ОС свойственны следующие особенности:

- клиентские ОС функционируют на рабочих станциях в интересах конечных пользователей;
- рабочие станции, работающие под управлением клиентских ОС, могут быть автономными (не подключенными в сеть), могут быть объединены в одноранговую сеть и работать в составе рабочей группы, либо могут быть объединены в сеть с централизованным управлением со стороны серверов с установленными и соответствующим образом настроенными серверными ОС;
- на рабочих станциях, функционирующих под управлением клиентских ОС, может устанавливаться ПО пользователей, а также клиентская часть клиент-серверных приложений.

В случае взаимодействия ОО с другими ОС при объединении в рабочую группу, ОО располагает своим независимым набором атрибутов безопасности для всех сущностей в пределах ОДФ и независимыми возможностями по управлению используемыми аппаратными средствами.

В случае взаимодействия ОО с другими ОС при подключении соответствующей рабочей станции в сеть с централизованным управлением со стороны серверов, возможна организация централизованного управления атрибутами безопасности для всех сущностей в пределах ОДФ и централизованного управления используемыми аппаратными средствами.

2.2 Основные функциональные возможности ОО

2.2.1 Основные функциональные возможности обеспечения функционирования

Управление процессами

Важнейшей частью ОО, непосредственно влияющей на функционирование рабочей станции пользователя, является подсистема управления процессами.

Для каждого вновь создаваемого процесса ОО генерирует системные информационные структуры, которые содержат данные о потребностях процесса в ресурсах вычислительной системы, а также о фактически выделенных ему ресурсах.

Чтобы процесс мог быть выполнен, ОО должен назначить ему область оперативной памяти, в которой будут размещены коды и данные процесса, а также предоставить ему необходимое количество процессорного времени. Кроме того, процессу может понадобиться доступ к таким ресурсам, как файлы и устройства ввода-вывода.

В информационные структуры процесса включаются вспомогательные данные, характеризующие историю функционирования процесса в ОО (например, доля времени потраченная на операции ввода-вывода, на вычисления и т.п.), его текущее состояние (активное или заблокированное), степень привилегированности процесса (значение приоритета). Подобные данные учитываться ОО при принятии решения о предоставлении ресурсов процессу.

В ОО одновременно может существовать несколько процессов. Часть процессов, порождаемых по инициативе пользователей и их приложений, выступает в роли пользовательских процессов. Другая часть процессов, выступающих в роли системных, инициализируется самим ОО для выполнения своих функций.

Процессы одновременно претендуют на использование одних и те же ресурсов, и ОО осуществляет поддержание очередей заявок процессов на ресурсы, например очереди к процессору, к принтеру, к последовательному порту.

Важной задачей ОО является защита ресурсов, выделенных данному процессу, от остальных процессов. Одним из защищаемых ресурсов процесса являются области оперативной памяти, в которой хранятся коды и данные процесса. Совокупность всех областей оперативной памяти, выделенных ОО процессу, называется его адресным пространством, и каждый процесс работает в своем адресном пространстве.

На протяжении периода существования процесса его выполнение может быть многократно прервано и продолжено. Для того чтобы возобновить выполнение процесса, необходимо восстановить состояние его операционной среды. Состояние операционной среды идентифицируется состоянием регистров и программного счетчика, режимом

работы процессора, указателями на открытые файлы, информацией о незавершенных операциях ввода-вывода, кодами ошибок выполняемых данным процессом системных вызовов и т. д. Эта информация называется контекстом процесса, при смене процесса происходит переключение контекстов.

Объект оценки осуществляет также функции синхронизации процессов, позволяющие процессу приостанавливать свое выполнение до наступления какого-либо события в системе, например завершения операции ввода-вывода, осуществляемой по его запросу ОО.

В ОО нет однозначного соответствия между процессами и программами. Один и тот же программный файл может породить несколько параллельно выполняемых процессов, а процесс может в ходе своего выполнения сменить программный файл и начать выполнять другую программу.

Таким образом, подсистема управления процессами планирует выполнение процессов, то есть распределяет процессорное время между несколькими одновременно существующими в системе процессами, осуществляет создание и уничтожение процессов, обеспечивает процессы необходимыми системными ресурсами, поддерживает синхронизацию процессов, а также обеспечивает взаимодействие между процессами.

Управление памятью

Память является для процесса таким же важным ресурсом, как и процессор, так как процесс может выполняться процессором только в том случае, если его коды и данные находятся в оперативной памяти.

Управление памятью включает распределение имеющейся физической памяти между всеми существующими в ОО в данный момент процессами, загрузку кодов и данных процессов в отведенные им области памяти, настройку адресно-зависимых частей кодов процесса на физические адреса выделенной области, а также защиту областей памяти каждого процесса.

В различных реализациях ОО существуют разные алгоритмы распределения памяти. Они могут отличаться, например, количеством выделяемых процессу областей памяти (в одних случаях память выделяется процессу в виде одной непрерывной области, а в других – в виде нескольких несмежных областей), степенью свободы границы областей (она может быть жестко зафиксирована на все время существования процесса или же динамически перемещаться при выделении процессу дополнительных объемов памяти). Также возможно распределение памяти посредством страниц фиксированного размера или сегментов переменной длины.

Одним из способов управления памятью в ОО является способ с использованием виртуальной памяти. Все данные, используемые программой, хранятся на диске и при необходимости частями (сегментами или страницами) отображаются в физическую память. При перемещении кодов и данных между оперативной памятью и диском подсистема виртуальной памяти выполняет трансляцию виртуальных адресов, полученных в результате компиляции и компоновки программы, в физические адреса ячеек оперативной памяти.

Средства защиты памяти, реализованные в ОО, пресекают несанкционированный доступ процессов к чужим областям памяти.

Таким образом, функциями ОО по управлению памятью являются отслеживание свободной и занятой памяти; выделение памяти процессам и освобождение памяти при завершении процессов; защита памяти; вытеснение процессов из оперативной памяти на диск, когда размеры основной памяти недостаточны для размещения в ней всех процессов, и возвращение их в оперативную память, когда в ней освобождается место, а также настройка адресов программы на конкретную область физической памяти.

Управление файлами и внешними устройствами

Объект оценки виртуализирует отдельный набор данных, хранящихся на внешнем накопителе, в виде файла — простой неструктурированной последовательности байтов, имеющей символьное имя. Для удобства работы с данными файлы группируются в каталоги, которые, в свою очередь, образуют группы — каталоги более высокого уровня. Пользователь может с помощью ОО выполнять над файлами и каталогами такие действия, как поиск по имени, удаление, вывод содержимого на внешнее устройство (например, на дисплей), изменение и сохранение содержимого.

Файловая система ОО выполняет преобразование символьных имен файлов, с которыми работает пользователь, в физические адреса данных на диске, организует совместный доступ к файлам, защищает их от несанкционированного доступа.

При выполнении своих функций файловая система тесно взаимодействует с подсистемой управления внешними устройствами, которая по запросам файловой системы осуществляет передачу данных между дисками и оперативной памятью.

Подсистема управления внешними устройствами, называемая также подсистемой ввода-вывода, исполняет роль интерфейса ко всем устройствам, подключенным к рабочей станции.

Программа, управляющая конкретной моделью внешнего устройства и учитывающая все его особенности, обычно называется драйвером этого устройства.

Драйвер может управлять единственной моделью устройства или же группой устройств определенного типа.

2.2.2 Основные функциональные возможности по предоставлению интерфейсов

Интерфейс прикладного программирования

Прикладные программисты используют в своих приложениях обращения к ОО, когда для выполнения тех или иных действий требуется особый статус, которым обладает только ОО. Например, действия, связанные с управлением аппаратными средствами рабочей станции, может выполнять только ОО. Помимо этих функций прикладной программист может воспользоваться набором сервисных функций ОО, которые упрощают разработку приложений. Функции такого типа реализуют универсальные действия, часто требующиеся в различных приложениях, такие, например, как обработка текстовых строк. Эти функции реализованы в виде отлаженных процедур, включенных в состав ОО. В то же время даже при наличии в ОО соответствующей функции она может быть реализована в рамках приложения.

Возможности ОО доступны разработчикам ПО в виде набора функций, называющегося интерфейсом прикладного программирования (Application Programming Interface, API). От конечного пользователя эти функции скрыты за оболочкой алфавитно-цифрового или графического пользовательского интерфейса.

Для разработчиков ПО все особенности конкретного ОО представлены особенностями его API. Поэтому ОО с различной внутренней организацией, но с одинаковым набором функций API для разработчика неразличимы, что упрощает стандартизацию ОО и обеспечивает переносимость приложений между внутренне различными ОО, соответствующими определенному стандарту на API.

Приложения выполняют обращения к функциям API с помощью системных вызовов. Способ, которым приложение получает услуги ОО, аналогичен вызову подпрограмм. Информация, требуемая ОО и состоящая обычно из идентификатора команды и данных, помещается в определенное место памяти, в регистры и/или стек. Затем управление передается ОО, который выполняет требуемую функцию и возвращает результаты через память, регистры или стеки. Если операция проведена неуспешно, то результат включает индикацию ошибки.

Способ реализации системных вызовов зависит от структурной организации ОО, которая, в свою очередь, тесно связана с особенностями аппаратной платформы. Кроме того, он зависит от языка программирования. При использовании ассемблера разработчик ПО устанавливает значения регистров и/или областей памяти, а затем выполняет

специальную инструкцию вызова сервиса или программного прерывания для обращения к некоторой функции ОО. При использовании языков высокого уровня функции ОО вызываются тем же способом, что и написанные пользователем подпрограммы, требуя задания определенных аргументов в определенном порядке.

Пользовательский интерфейс

Объект оценки обеспечивает удобный интерфейс не только для прикладных программ, но и для человека, работающего за терминалом. Этот человек может быть конечным пользователем, администратором ОО или программистом.

Объект оценки поддерживает развитые функции пользовательского интерфейса для интерактивной работы за терминалами двух типов: алфавитно-цифровыми и графическими.

При работе за алфавитно-цифровым терминалом пользователь имеет в своем распоряжении систему команд, мощность который отражает функциональные возможности данного ОО. Обычно командный язык ОО позволяет запускать и останавливать приложения, выполнять различные операции с файлами и каталогами, получать информацию о состоянии ОО (количество работающих процессов, объем свободного пространства на дисках и т. п.), администрировать систему. Команды могут вводиться не только в интерактивном режиме с терминала, но и считываться из так называемого командного файла, содержащего некоторую последовательность команд.

Программный модуль ОО, ответственный за чтение отдельных команд или же последовательности команд из командного файла, выступает в роли командного интерпретатора.

Ввод команды может быть упрощен, если ОО поддерживает графический пользовательский интерфейс. В этом случае пользователь для выполнения нужного действия с помощью манипулятора выбирает на экране нужный пункт меню или графический символ.

2.2.3 Основные функциональные возможности обеспечения безопасности

Аудит безопасности

Объект оценки обеспечивает выявление и запись данных о событиях, существенных с точки зрения безопасности, а также предоставляет средства для анализа записей о таких событиях. Перечень типов событий, подлежащих регистрации, определяется администратором и может детализироваться вплоть до доступа отдельных пользователей или групп к конкретным файлам или каталогам. После настройки

параметров аудита возможно отслеживание доступа пользователей к определенным объектам и анализ недостатков в настройке параметров безопасности. Записи аудита, содержащие сведения по выбранным событиям, содержат информацию о пользователе, который был инициатором события и выполнял какие-либо действия в отношении контролируемого объекта, а также дату, время события и другие данные. ОО обеспечивает возможность доступа к журналу аудита только уполномоченным на это пользователям.

Защита данных

Объект оценки реализует политику дискреционного управления доступом. ФБО обеспечивают опосредованный доступ между субъектами (пользовательскими процессами) и объектами данных пользователя (именованными объектами). Решение о доступе принимается на основе сравнительного анализа атрибутов безопасности, связанных с запрашивающим субъектом, и атрибутов безопасности, связанных с объектом, к которому осуществляется доступ. Атрибуты безопасности субъекта включают идентификатор пользователя, идентификаторы групп, членами которых является данный пользователь, и назначенные привилегии. Атрибуты объекта включают идентификатор владельца данного объекта и список управления доступом, содержащий строки, определяющие права, предоставленные конкретному пользователю или группе для данного объекта. Изменять атрибуты безопасности могут пользователи, которым даны соответствующие права. Помимо реализации политики дискреционного управления доступом ОО также обеспечивает защиту данных посредством механизма, обеспечивающего обезличивание (обнуление) остаточной информации в свободных блоках памяти (оперативной и дисковой) перед их предоставлением каким-либо процессам, выполняющимся в режиме пользователя.

Идентификация и аутентификация

Объект оценки обеспечивает уникальную идентификацию и аутентификацию пользователей при входе в ОО, требуя ввести идентификатор пользователя и пароля. Идентификация и аутентификация осуществляются до выполнения пользователем каких-либо действий. ОО поддерживает аутентификацию пользователей вместе с их авторизацией. Авторизация пользователей представляет начальный уровень для разрешения доступа к локальным и сетевым ресурсам. При входе пользователя в ОО для безопасной передачи его идентификационной и аутентификационной информации предоставляется доверенный маршрут. ОО предоставляет механизм блокирования учетной записи пользователя после определенного количества попыток ввода

неправильного имени и/или пароля пользователя до ее разблокирования администратором или по истечению времени действия, заданного для счетчика блокировки.

Защита функций безопасности ОО

Объект оценки предоставляет ряд возможностей для обеспечения защиты функций безопасности ОО. Изоляция процессов и поддержания домена безопасности обеспечивают безопасное выполнение функций безопасности ОО. Возможность осуществления периодического тестирования среды функционирования ОО (аппаратной части) обеспечивает поддержание уверенности в целостности и корректности функционирования ФБО.

3 Среда безопасности ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

- предположений относительно аспектов безопасности среды ОО;
- угроз безопасности, которым нужно противостоять средствами ОО;
- политики безопасности организации, которой должен следовать ОО.

3.1 Предположения безопасности

Для среды ОО необходимо обеспечить выполнение следующих условий.

Предположения о взаимодействии

A.Connect

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемых помещениях.

A.Peer

К системам, с которыми ОО взаимодействует, должна быть применена идентичная ОО политика безопасности.

Предположения о персонале

A.Coop

Уполномоченные для доступа к ОО пользователи должны пройти проверку на благонадежность, их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

A.Manage

Управление безопасным функционированием ОО должны осуществлять лица, прошедшие проверку на компетентность.

A.No_Evil_Adm

Персонал, ответственный за выполнение администрирования ОО, должен пройти проверку на благонадежность и в своей деятельности должен руководствоваться соответствующей документацией.

Предположения о физической защите

A.Locate

Для предотвращения несанкционированного физического доступа вычислительные ресурсы, используемые ОО, должны располагаться в контролируемой зоне.

A.Protect

Критичное с точки зрения обеспечения безопасности аппаратное обеспечение, на базе которого функционирует ОО, и программное обеспечение ОО должно быть защищено от несанкционированной физической модификации.

3.2 Угрозы

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

T.Audit_Corrupt

Модификация или удаление данных аудита неуполномоченными на это пользователями в нарушение политики безопасности.

T.Config_Corrupt

Модификация конфигурационных данных неуполномоченными на это пользователями в нарушение политики безопасности.

T.Objects_Not_Clean

Несанкционированный доступ пользователей к информации вследствие отсутствия надлежащих механизмов очистки информационного содержания освобождаемых совместно используемых объектов доступа.

T.Spoof

Хищение аутентификационных данных уполномоченных пользователей путем подмены сервисов доступа.

T.Sysacc

Несанкционированный доступ к ОО уполномоченного пользователя под видом администратора или другого уполномоченного пользователя и действия от их имени

путем использования недостатков механизмов разграничения доступа с целью нарушения функционирования ОО или ограничения доступа к ОО.

T.Unauth_Access

Доступ к системным данным со стороны неуполномоченных пользователей вследствие недостатков механизмов разграничения доступа.

T.Unauth_Modification

Несанкционированный доступ к ОО и пользовательским данным путем модификации функций безопасности ОО вследствие недостатков механизмов защиты функций безопасности ОО.

T.Undetected_Actions

Невыполнение регистрации несанкционированных действий вследствие недостатков механизмов аудита.

T.User_Corrupt

Модификация пользовательских данных неуполномоченными на это пользователями вследствие недостатков механизмов ограничения доступа к данным, осуществляемого уполномоченными пользователями.

3.3 Политика безопасности организации

Объект оценки должен следовать приведенным ниже правилам политики безопасности организации.

P.Accountability

Пользователи ОО должны быть подотчетны за свои действия в пределах ОО.

P.Authorized_Users

Доступ к ОО должен быть возможен только уполномоченным на доступ к ОО пользователям.

P.Need_To_Know

Объект оценки должен ограничивать доступ к информации, возможность модификации и удаления информации в защищаемых ресурсах в соответствии со служебными обязанностями пользователей.

P.Authorization

Объект оценки должен иметь возможность ограничивать уровень полномочий для каждого пользователя.

4 Цели безопасности

4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

O.Authorization

ФБО должны обеспечивать доступ к ОО и защищаемым ресурсам только уполномоченным на это пользователям.

O.Discretionary_Access

ФБО должны осуществлять разграничение доступа к ресурсам, основанное на идентификаторах пользователей. ФБО должны давать возможность уполномоченным пользователям определять доступность защищаемых ресурсов для других пользователей.

O.Auditing

ФБО должны осуществлять регистрацию относящихся к безопасности ОО действий пользователей. ФБО должны предоставлять данные регистрации уполномоченным администраторам.

O.Residual_Information

ФБО должны обеспечивать недоступность информационного содержания освобождаемых защищаемых ресурсов.

O.Manage

ФБО должны предоставлять все необходимые функции и средства в поддержку уполномоченным администраторам, ответственным за управление безопасностью ОО.

O.Enforcement

ФБО должны быть спроектированы и реализованы таким образом, чтобы обеспечивалось осуществление политики безопасности организации в среде функционирования.

O.Audit_Protection

ФБО должны обеспечивать защиту данных аудита, содержащих информацию о действиях пользователей.

O.Protect

В целях защиты от внешнего воздействия ФБО должны обеспечивать защиту собственных данных, поддерживая домен для своего функционирования.

O.Trusted_Path

ФБО должны обеспечивать невозможность подмены сервисов доступа на этапе аутентификации пользователей.

O.Limit_Authorization

ФБО должны предоставлять возможность ограничивать уровень полномочий для каждого пользователя.

4.2 Цели безопасности для среды

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

O.Install

Ответственные за ОО лица должны обеспечить поставку, установку, управление и функционирование ОО в соответствии с руководствами.

O.Physical

Ответственные за ОО лица должны обеспечить защиту критичных по безопасности частей ОО от физического воздействия, способного скомпрометировать цели безопасности.

O.Creden

Ответственные за ОО лица должны обеспечивать мероприятия по защите всей удостоверяющей информацией (пароли или другая аутентификационная информация).

5 Требования безопасности ИТ

В данном разделе ПЗ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из части 2 ОК. Требования доверия основаны на компонентах требований доверия из части 3 ОК и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД1, усиленного компонентом доверия AVA_SOF.1 (Оценка стойкости функции безопасности ОО). В качестве минимального уровня стойкости функций безопасности, реализованных вероятностными или перестановочными механизмами, заявлена средняя СФБ.

5.1 Функциональные требования безопасности ОО

Функциональные требования безопасности ОО включают функциональный пакет, содержащий ФТБ, определенные в ПЗ "Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999". Кроме того, в настоящем ПЗ определены дополнительные (по отношению к упомянутым выше) ФТБ, исходя из специфики ОО "Клиентская операционная система".

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности ОО, приведены в таблице 5.1.

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО.

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
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_RIP.2	Полная защита остаточной информации
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов

Идентификатор компонента требований	Название компонента требований
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.2	Идентификация до любых действий пользователя
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 ФБО
FMT_MTD.2	Управление ограничениями данных ФБО
FMT_REV.1	Отмена
FMT_SAE.1	Ограниченная по времени авторизация
FMT_SMR.1	Роли безопасности
FMT_SMR.3	Принятие ролей
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени
FRU_RSA.1	Максимальные квоты
FTA_SSL.1	Блокирование сеанса, инициированное ФБО
FTA_SSL.2	Блокирование, инициированное пользователем
FTA_TSE.1	Открытие сеанса с ОО
FTP_TRP.1	Доверенный маршрут

5.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

а) запуск и завершение выполнения функций аудита;

б) **(события, приведенные во втором столбце таблицы 5.2)**.

FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ/ЗБ, [информацию, определенную в третьем столбце таблицы 5.2].

Зависимости: FPT_STM.1 Надежные метки времени

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_SAR.1	Чтение информации из записей аудита	
FAU_SAR.2	Неуспешные попытки читать информацию из записей аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время сбора данных аудита	
FAU_STG.3	Предпринимаемые действия после превышения порога заполнения	
FAU_STG.4	Предпринимаемые действия при сбое хранения журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на объекте, на который распространяется ПФБ	Идентификатор объекта
FIA_AFL.1	Блокирование учетной записи в результате превышения максимального числа неуспешных попыток входа в систему	
FIA_SOS.1	Отклонение или принятие ФБО любого проверенного секрета	
FIA_UAU.2	Все случаи использования механизма аутентификации	
FIA_UID.2	Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	
FIA_USB.1	Успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта)	
FMT_MOF.1	Все модификации политики аудита	
FMT_MSA.1	Все модификации значений атрибутов безопасности	
FMT_MSA.3	Модификации настройки по умолчанию разрешающих или ограничительных правил. Все модификации начальных значений атрибутов безопасности	
FMT_MTD.1 (1)	Все модификации значений данных ФБО	
FMT_MTD.1 (2)	Все модификации значений данных ФБО	Новое значение данных ФБО
FMT_MTD.1 (3)	Все модификации значений данных ФБО	Новое значение данных ФБО
FMT_MTD.1 (4)	Все модификации значений данных ФБО	
FMT_MTD.1 (5)	Все модификации значений данных ФБО	
FMT_MTD.2	Все модификации ограничений данных ФБО. Все модификации действий, предпринимаемых при нарушениях	

Компонент	Событие	Детализация
	ограничений	
FMT_REV.1 (1)	Все попытки отменить атрибуты безопасности	
FMT_REV.1 (2)	Все попытки отменить атрибуты безопасности	
FMT_SAE.1	Назначение срока действия для атрибута. Действия, предпринятые по истечении назначенного срока	
FMT_SMR.1	Модификация группы пользователей – исполнителей роли. Каждое использование прав, предоставляемых ролью	Роль и начало запроса
FPT_AMT.1	Выполнение тестирования базовой машины и результаты тестирования	
FPT_STM.1	Изменения внутреннего представления времени	
FTA_SSL.1	Все попытки разблокирования интерактивного сеанса	
FTA_TSE.1	Все попытки открытия сеанса пользователя	
FTP_TRP.1	Попытки аутентификации и разблокирования	

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

Зависимости: FAU_GEN.1 Генерация данных аудита
FIA_UID.1 Выбор момента идентификации

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченным администраторам] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

Зависимости: FAU_GEN.1 Генерация данных аудита

FAU_SAR.2 Ограниченный просмотр аудита

FAU_SAR.2.1 ФБО должны запретить всем пользователям доступ к чтению записей аудита, за исключением пользователей, 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 выполнить [выбор: *поиск, сортировка, упорядочение*] данных аудита, основанный на

[

следующих атрибутах:

а) идентификатор пользователя;

б) [назначение: список дополнительных атрибутов, на которых основана избирательность аудита]

].

Зависимости: FAU_SAR.1 Просмотр аудита

FAU_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:

а) *идентификатор пользователя;*

б) [назначение: *список дополнительных атрибутов, на которых основана избирательность аудита*].

Зависимости: FAU_GEN.1 Генерация данных аудита

FMT_MTD.1 Управление данными ФБО

FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.1.1 ФБО должны защищать хранимые записи аудита от несанкционированного удаления.

FAU_STG.1.2 ФБО должны быть способны к *предотвращению* модификации записей аудита.

Зависимости: FAU_GEN.1 Генерация данных аудита

FAU_STG.3 Действия в случае возможной потери данных аудита

FAU_STG.3.1 ФБО должны выполнить [формирование предупреждения уполномоченному администратору], если журнал аудита превышает [назначение: *принятое ограничение*].

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны выполнить *предотвращение событий, подвергающихся аудиту, исключая предпринимаемые уполномоченным* ***администратором***, и [назначение: *другие действия, которые нужно предпринять в случае возможного сбоя хранения журнала аудита*] при переполнении журнала аудита.

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита

5.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] для

[

а) [назначение: *список субъектов*], действующих от имени пользователей;

б) [назначение: *список именованных объектов*];

в) всех операций между субъектами и объектами

].

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

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] к объектам, основываясь на

[

следующем:

а) ассоциированные с субъектом идентификатор пользователя и принадлежность к группе (группам);

б) следующие, ассоциированные с объектом, атрибуты управления доступом [назначение: *список атрибутов управления доступом, которые должны обеспечить возможность:*

- *ассоциировать разрешение или запрет на выполнение операций с идентификаторами одного или более пользователей;*
- *ассоциировать разрешение или запрет на выполнение операций с идентификаторами одной или более групп;*

- *ассоциировать разрешение или запрет на выполнение операций по умолчанию*]

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: [назначение: *набор правил, определяющих политику дискреционного доступа, в которых:*

а) для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда идентификатор субъекта соответствует идентификатору, определенному в атрибутах контроля доступа объекта;

б) для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда субъект принадлежит группе, идентификатор которой, определен в атрибутах контроля доступа объекта;

в) для каждой операции должно быть определено правило или правила использования атрибутов разрешения по умолчанию в случаях, когда идентификатор субъекта не соответствует определенному в атрибутах контроля доступа объекта и субъект принадлежит группе, идентификатор которой, не определен в атрибутах контроля доступа объекта

].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: [назначение: *правила, основанные на атрибутах безопасности, которые явно разрешают доступ субъектов к объектам*].

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

Зависимости: FDP_ACC.1 Ограниченное управление доступом

FMT_MSA.3 Инициализация статических атрибутов

FDP_RIP.2 Полная защита остаточной информации

FDP_RIP.2.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при *распределении ресурсов* для всех объектов.

Зависимости: отсутствуют.

Замечание по применению:

В случае, когда субъект является предметом операций (например, при установлении связи между процессами), над субъектом производятся действия аналогичные как над объектом, т.е. обеспечение недоступности информационного содержания при распределении, и процессы в таком случае выступают в роли объектов.

5.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [определенное уполномоченным администратором число] неуспешных попыток аутентификации, относящихся к [назначение: *список событий аутентификации*].

FIA_AFL.1.2 При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить [назначение: *список действий*].

Зависимости: FIA_UAU.1 Выбор момента аутентификации

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

[

а) идентификатор пользователя;

б) принадлежность к группе;

в) аутентификационные данные;

г) имеющие отношение к безопасности роли;

д) [назначение: *другие атрибуты безопасности пользователя*]

].

Зависимости: отсутствуют.

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 ФБО должны предоставить механизм для верификации того, что секреты отвечают

[

следующему:

а) для каждой попытки использования механизма аутентификации вероятность случайного доступа должна быть меньше, чем 10^{-6};

б) при неоднократных попытках использования механизма аутентификации в течение одной минуты вероятность случайного доступа должна быть меньше, чем 10^{-5};

в) обратная связь при использовании механизма аутентификации не должна приводить к повышению вероятностей вышеупомянутых метрик

].

Зависимости: отсутствуют.

FIA_UAU.2 Аутентификация до любых действий пользователя

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

Зависимости: FIA_UID.1 Выбор момента идентификации

FIA_UAU.7 Аутентификация с защищенной обратной связью

FIA_UAU.7.1 ФБО должны предоставлять пользователю только [обратную связь в скрытом виде] во время выполнения аутентификации.

Зависимости: FIA_UAU.1 Выбор момента аутентификации

FIA_UID.2 Идентификация до любых действий пользователя

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

Зависимости: отсутствуют.

FIA_USB.1 Связывание пользователь-субъект

FIA_USB.1.1 ФБО должны ассоциировать **следующие** атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя**:**

а) идентификатор пользователя, который ассоциируется с возможными для аудита событиями;

б) идентификатор или идентификаторы пользователя, используемые для осуществления политики дискреционного управления доступом;

в) принадлежность к группе или группам, используемая для осуществления политики дискреционного управления доступом;

г) [назначение: *любые другие атрибуты безопасности пользователя*].

FIA_USB.1.2 ФБО должны устанавливать следующие правила начальной ассоциации атрибутов безопасности пользователя с субъектами, действующими от имени пользователя:

а) [назначение: *правила начальной ассоциации*].

FIA_USB.1.3 ФБО должны устанавливать следующие правила, определяющие возможность изменения атрибутов безопасности пользователя, ассоциированных с субъектами, действующими от имени пользователя:

а) [назначение: *правила изменения атрибутов*].

Зависимости: FIA_ATD.1 Определение атрибутов пользователя

5.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставить** возможность [выбор: *определение режима выполнения, отключение, подключение, модификация режима выполнения*] функций **связанных с:**

[

а) аудитом;

б) [назначение: *другие функции*]

]

только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 Роли безопасности

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** возможность *модификации* [атрибутов

управления доступом, ассоциированных с именованным объектом] только [назначение: *уполномоченные идентифицированные роли*].

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

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** *ограничительные* значения по умолчанию для атрибутов безопасности, которые используются для осуществления **политики дискреционного управления доступом**.

FMT_MSA.3.2 ФБО должны предоставить возможность [назначение: *уполномоченные идентифицированные роли*] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

Зависимости: FMT_MSA.1 Управление атрибутами безопасности
FMT_SMR.1 Роли безопасности

FMT_MTD.1 (1) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *удаления, очистки, [создания]* [журнала аудита] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 Роли безопасности

Замечания по применению:

Выбранные функции «создание, удаление и очистка» для управления журналом аудита являются общими функциями управления. Любые другие функции управления аудитом, необходимые для частного применения механизма аудита, должны определяться в ЗБ.

FMT_MTD.1 (2) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *модификации или [просмотра]* [множества подвергающихся аудиту событий] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 Роли безопасности

Замечания по применению:

Множество подвергающихся аудиту событий является подмножеством событий, потенциально подвергаемых аудиту с помощью ФБО.

Важный аспект аудита состоит в том, что пользователи не способны влиять на отслеживание аудитом их действий, не должны знать о выборе событий для фиксации и управлять аудитом.

FMT_MTD.1 (3) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *модификации и [инициализации]* [атрибутов безопасности пользователя, кроме аутентификационных данных] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 Роли безопасности

FMT_MTD.1 (4) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *[инициализации]* [аутентификационных данных] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 Роли безопасности

FMT_MTD.1 (5) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *модификации* [аутентификационных данных] только

[

следующим:

а) уполномоченным администраторам;

б) пользователям, уполномоченным модифицировать собственные аутентификационные данные

].

Зависимости: FMT_SMR.1 Роли безопасности

Замечания по применению:

Аутентификационные данные пользователь должен предоставить ФБО, к ним относятся, например, пароли, персональные идентификационные номера, биометрические характеристики и т.п.

Этот компонент не требует, чтобы любой пользователь был уполномочен изменять собственную информацию аутентификации, компонент только устанавливает разрешение на это действие. Нет необходимости в том, чтобы запросы на изменение данных аутентификации требовали повторной аутентификации.

FMT_MTD.2 Управление ограничениями данных ФБО

FMT_MTD.2.1 ФБО должны предоставить возможность определения ограничений для [порогового значения количества неуспешных попыток аутентификации] только [уполномоченным администраторам].

FMT_MTD.2.2 ФБО должны предпринять следующие действия при достижении или превышении данными ФБО установленных выше ограничений: [ФБО должны блокировать учетную запись пользователя на время, определенное уполномоченным администратором].

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

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны **предоставить** возможность отмены атрибутов безопасности, ассоциированных с *пользователями* в пределах ОДФ только [уполномоченным администраторам].

FMT_REV.1.2 ФБО должны реализовать правила

[

а) немедленной отмены имеющих отношение к безопасности полномочий;

б) [назначение: *список других правил отмены, относящихся к пользователям*]

].

Зависимости: FMT_SMR.1 Роли безопасности

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны **предоставить** возможность отмены атрибутов безопасности, ассоциированных с *объектами* в пределах ОДФ только [пользователям, уполномоченным на изменение атрибутов безопасности в соответствии с политикой дискреционного управления доступом].

FMT_REV.1.2 ФБО должны реализовать правила

[

а) права доступа, ассоциированные с объектом, должны быть установлены после проведения проверки доступа;

б) [назначение: *список других правил отмены, относящихся к объектам*]

].

Зависимости: FMT_SMR.1 Роли безопасности

FMT_SAE.1 Ограниченная по времени авторизация

FMT_SAE.1.1 ФБО должны **предоставить** возможность назначать срок действия для [аутентификационных данных] только [уполномоченным администраторам].

FMT_SAE.1.2 Для каждого из этих атрибутов безопасности ФБО должны быть способны к [блокированию ассоциированной с пользователем учетной записи] по истечении ее срока действия.

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

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[

а) уполномоченный администратор;

б) пользователи, уполномоченные согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта;

в) пользователи, уполномоченные модифицировать собственные аутентификационные данные;

г) [назначение: другие роли]

].

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

Зависимости: FIA_UID.1 Выбор момента идентификации

FMT_SMR.3 Принятие ролей

FMT_SMR.3.1 ФБО должны требовать точный запрос для принятия следующих ролей [уполномоченный администратор].

Зависимости: FMT_SMR.1 Роли безопасности

5.1.5 Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ [выбор: *при первоначальном запуске, периодически во время нормального функционирования, по запросу уполномоченного пользователя, при других условиях*] для демонстрации правильности выполнения предположений

безопасности, обеспечиваемых абстрактной машиной, которая положена в основу ФБО.

Зависимости: отсутствуют.

Замечания по применению:

Этот компонент относится к обеспечению функционирования аппаратного обеспечения ОО. Пакет тестовых программ необходим для охвата аспектов функционирования аппаратного обеспечения, от которых зависит выполнение требуемых функций из числа ФБО, включая отделение домена ФБО. Если сбои аппаратного обеспечения не приводят к компрометации функций из числа ФБО, то тестирование относительно таких сбоев не требуется.

FPT_RVM.1 Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБО должны быть способны предоставить надежные метки времени для собственного использования.

Зависимости: отсутствуют.

5.1.6 Доступ к ОО (FTA)

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

FTA_SSL.1.1 ФБО должны блокировать интерактивный сеанс после [истечения интервала времени бездействия выбранного пользователя], 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].

Зависимости: FIA_UAU.1 Выбор момента аутентификации

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса, основываясь на [истечении срока действия аутентификационных данных].

Зависимости: отсутствуют.

5.1.7 Доверенный маршрут/канал (FTP)

FTP_TRP.1 Доверенный маршрут

FTP_TRP.1.1 ФБО должны предоставлять маршрут связи между собой и *локальным* пользователем, который логически отличим от других маршрутов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту передаваемых данных от модификации или раскрытия.

FTP_TRP.1.2 ФБО должны позволить *локальным пользователям* инициировать связь через доверенный маршрут.

FTP_TRP.1.3 ФБО должны требовать использования доверенного маршрута для *начальной аутентификации пользователя,* [назначение: *другие услуги, для которых требуется доверенный маршрут*].

Зависимости: отсутствуют.

5.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 ОК и образуют ОУД1, усиленный компонентом AVA_SOF.1 (см. таблицу 5.3).

Таблица 5.3 – Требования доверия к безопасности ОО

Класс доверия	Идентификатор компонентов доверия	Название компонентов доверия
Управление конфигурацией	ACM_CAP.1	Номера версий
Поставка и эксплуатация	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_RCR.1	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО

5.2.1 Управление конфигурацией (ACM)

ACM_CAP.1 Номера версий

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

ACM_CAP.1.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

ACM_CAP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.2.2 Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

ADO_IGS.1.1D Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

Элементы содержания и представления свидетельств

ADO_IGS.1.1C Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.

Элементы действий оценщика

ADO_IGS.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1.2E Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

5.2.3 Разработка (ADV)

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_FSP.1.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.1.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.1.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

ADV_FSP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.1.2E Оценщик должен сделать независимое заключение, что функциональная спецификация – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_RCR.1.1D Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

ADV_RCR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.2.4 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

AGD_ADM.1.1D Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования.

Элементы содержания и представления свидетельств

AGD_ADM.1.1C Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.

AGD_ADM.1.2C Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.

AGD_ADM.1.3C Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_ADM.1.4C Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.

AGD_ADM.1.5C Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.

AGD_ADM.1.6C Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением

обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.

AGD_ADM.1.7C Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_ADM.1.8C Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.

Элементы действий оценщика

AGD_ADM.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

AGD_USR.1.1C Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.

AGD_USR.1.2C Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.

AGD_USR.1.3C Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_USR.1.4C Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.

AGD_USR.1.5C Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_USR.1.6C Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.

Элементы действий оценщика

AGD_USR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.2.5 Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ATE_IND.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.1.2E Оценщик должен протестировать необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

5.2.6 Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

AVA_SOF.1.1D Разработчик должен выполнить анализ стойкости функции безопасности ОО для каждого механизма, идентифицированного в ЗБ как имеющего утверждение относительно стойкости функции безопасности ОО.

Элементы содержания и представления свидетельств

AVA_SOF.1.1C Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.

AVA_SOF.1.2C Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ/ЗБ.

Элементы действий оценщика

AVA_SOF.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_SOF.1.2E Оценщик должен подтвердить, что утверждения относительно стойкости корректны.

6 Обоснование

В данном разделе дано логическое обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ПЗ.

6.1 Логическое обоснование целей безопасности

6.1.1 Логическое обоснование целей безопасности для ОО

В таблице 6.1 приведено отображение целей безопасности на угрозы и политику безопасности.

Таблица 6.1 – Отображение целей безопасности на угрозы и политику безопасности организации

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Audit_Protection	O.Residual_Information	O.Manage	O.Enforcement	O.Protect	O.Trusted_Path	O.Limit_Authorization
T.Audit_Corrupt				X						
T.Config_Corrupt								X		
T.Objects_Not_Clean					X					
T.Spoof									X	
T.Sysacc	X									
T.Unauth_Access	X							X		
T.Unauth_Modification								X		
T.Undetected_Actions			X							
T.User_Corrupt		X						X		
P.Accountability			X			X	X			
P.Authorized_Users	X					X	X			
P.Need_To_Know		X			X	X	X			
P.Authorization										X

O.Authorization

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.Sysacc** и **T.Unauth_Access** и реализацией политики безопасности **P.Authorized_Users**, так как обеспечивает защиту ОО и его ресурсов от несанкционированного доступа и обеспечивает возможность доступа к ОО и его ресурсам только уполномоченным пользователям.

O.Discretionary_Access

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.User_Corrupt**, и реализацией политики безопасности **P.Need_To_Know**, так как обеспечивает возможность уполномоченным пользователям определять доступность ресурсов для других пользователей и в соответствии с этим осуществлять разграничение доступа к ресурсам.

O.Auditing

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.Undetected_Actions**, и реализацией политики безопасности **P.Accountability**, так как обеспечивает регистрацию относящихся к безопасности ОО действий пользователей и предоставление данных регистрации уполномоченным администраторам. Достижение цели обеспечивает невозможность необнаружения неуполномоченных действий и позволяет обеспечить подотчетность пользователей.

O.Audit_Protection

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.Audit_Corrupt**, так как обеспечивает предотвращение утраты и несанкционированного доступа к данным аудита.

O.Residual_Information

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.Objects_Not_Clean**, и реализацией политики безопасности **P.Need_To_Know**, так как обеспечивает недоступность информационного содержания освобождаемых защищаемых ресурсов и предотвращает использование остаточной информации при доступе к ресурсам нескольких пользователей.

O.Manage

Достижение этой цели безопасности необходимо в связи с реализацией политик безопасности **P.Accountability, P.Authorized_Users, P.Need_To_Know** так как обеспечивает предоставление необходимых функций и средств в поддержку уполномоченным администраторам, ответственным за управление безопасностью ОО, в том числе поддержку управления аудитом, защиты ресурсов и защиты доступа в систему.

O.Enforcement

Достижение этой цели безопасности необходимо в связи с реализацией политик безопасности **P.Accountability, P.Authorized_Users, P.Need_To_Know** так как обеспечивает корректность функционирования ФБО.

O.Protect

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.Config_Corrupt, T.Unauth_Access, T.Unauth_Modification**, так как обеспечивает защиту ФБО от внешнего воздействия и предотвращает несанкционированный доступ к данным ФБО.

O.Trusted_Path

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.Spoof**, так как обеспечивает невозможность подмены сервисов доступа на этапе аутентификации пользователей.

O.Limit_Authorization

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.Authorization,** так как обеспечивает возможность ограничения уровня полномочий пользователей.

6.1.2 Логическое обоснование целей безопасности для среды

В таблице 6.2 приведено отображение целей безопасности на угрозы и политику безопасности.

Таблица 6.2 – Отображение целей безопасности для среды на предположения безопасности.

	O.Install	O.Physical	O.Creden
A.Connect		**X**	
A.Peer	**X**		
A.Coop			**X**
A.Manage	**X**		
A.No_Evil_Adm	**X**		
A.Locate		**X**	
A.Protect		**X**	

O.Install

Достижение этой цели безопасности необходимо в связи с реализацией предположений безопасности **A.Peer, A.Manage, A.No_Evil_Adm,** так как обеспечивает безопасные поставку, установку, управление и функционирование ОО компетентными администраторами в соответствии с документацией.

O.Physical

Достижение этой цели безопасности необходимо в связи с реализацией предположений безопасности **A.Connect, A.Locate,** так как обеспечивает защиту ОО от несанкционированного физического воздействия.

O.Creden

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Coop,** так как обеспечивает выполнения надлежащих мероприятий по защите удостоверяющей информации.

6.2 Логическое обоснование требований безопасности

6.2.1 Логическое обоснование функциональных требований безопасности

В таблице 6.3 представлено отображение функциональных требований безопасности на цели безопасности ОО.

Таблица 6.3 – Отображение функциональных требований безопасности на цели безопасности

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Audit_Protection	O.Residual_Information	O.Manage	O.Enforcement	O.Protect	O.Trusted_Path	O.Limit_Authorization
FAU_GEN.1			X							
FAU_GEN.2			X							
FAU_SAR.1			X			X				
FAU_SAR.2			X							
FAU_SAR.3			X			X				
FAU_SEL.1			X			X				
FAU_STG.1			X	X						
FAU_STG.3			X			X				
FAU_STG.4			X	X		X				
FDP_ACC.1		X								
FDP_ACF.1		X								
FDP_RIP.2					X					
FIA_AFL.1	X									
FIA_ATD.1	X	X								X
FIA_SOS.1	X									
FIA_UAU.2	X									
FIA_UAU.7	X									
FIA_UID.2	X									
FIA_USB.1		X	X							
FMT_MOF.1						X				
FMT_MSA.1		X				X				
FMT_MSA.3		X				X				
FMT_MTD.1 (1)			X			X				
FMT_MTD.1 (2)			X			X				
FMT_MTD.1 (3)						X		X		
FMT_MTD.1 (4)	X					X				
FMT_MTD.1 (5)	X					X				

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Audit_Protection	O.Residual_Information	O.Manage	O.Enforcement	O.Protect	O.Trusted_Path	O.Limit_Authorization
FMT_MTD.2	**X**					**X**				
FMT_REV.1 (1)						**X**				**X**
FMT_REV.1 (2)		**X**								
FMT_SAE.1	**X**					**X**				
FMT_SMR.1						**X**				**X**
FMT_SMR.3						**X**				
FPT_AMT.1								**X**		
FPT_RVM.1							**X**			
FPT_SEP.1							**X**	**X**		
FPT_STM.1			**X**							
FTA_SSL.1	**X**									
FTA_TSE.1	**X**									
FTP_TRP.1									**X**	

FAU_GEN.1 Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита и события, которые должны подвергаться аудиту. Рассматриваемый компонент сопоставлен с целью **O.Auditing** и способствует ее достижению.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение требований данного компонента позволяет ассоциировать события, подвергаемые аудиту с идентификатором пользователя. Рассматриваемый компонент сопоставлен с целью **O.Auditing** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность прочтения всей информации аудита, которая для уполномоченного администратора является понятной. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает, что данные аудита недоступны для чтения неуполномоченным пользователям. Рассматриваемый компонент сопоставлен с целью **O.Auditing** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает возможность выполнения поиска и сортировки уполномоченным администратором данных аудита, основанных на определенных атрибутах. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий подвергающихся аудиту уполномоченным администратором по определенным атрибутам. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает защиту журнала аудита от несанкционированного изменения. При этом доступ к журналу аудита разрешен только уполномоченному администратору. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Audit_Protection** и способствует их достижению.

FAU_STG.3 Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает формирование предупреждения уполномоченному администратору в случае превышения журналом аудита определенного размера. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает уполномоченному администратору возможность управления журналом аудита, когда последний становится полным. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Audit_Protection, O.Manage** и способствует их достижению.

FDP_ACC.1 Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает реализацию политики дискреционного доступа для субъектов, объектов доступа и всех операций между субъектами и объектами. Рассматриваемый компонент сопоставлен с целью **O.Discretionary_Access** и способствует ее достижению.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Выполнение требований данного компонента обеспечивает осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, определение правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **O.Discretionary_Access** и способствует ее достижению.

FDP_RIP.2 Полная защита остаточной информации

Выполнение требований данного компонента обеспечивает недоступность любого предыдущего информационного содержания ресурсов при их распределении для всех объектов. Рассматриваемый компонент сопоставлен с целью **O.Residual_Information** и способствует ее достижению.

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает ограничение попыток пройти процедуру аутентификации для лиц, не являющихся санкционированными пользователями. При достижении или превышении определенного уполномоченным администратором числа неуспешных попыток аутентификации некоторого лица, данное лицо лишается возможности предпринимать дальнейшие попытки пройти процедуру аутентификации. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержку для каждого пользователя списка атрибутов безопасности, в том числе и идентификатора пользователя. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Discretionary_Access, O.Limit_Authorization** и способствует их достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает предоставление механизма для верификации соответствия секретов определенным требованиям.

Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации санкционированного пользователя до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_UAU.7 Аутентификация с защищенной обратной связью

Выполнение требований данного компонента обеспечивает, что во время выполнения аутентификации пользователя обратная связь предоставляется в скрытом виде. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации пользователя до выполнения каких-либо действий от его имени и наступления каких-либо событий с ним связанных. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_USB.1 Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает выполнение ФБО ассоциирования атрибутов безопасности пользователя с субъектами, действующими от имени пользователя, установление правил начальной ассоциации и правил, определяющих возможность изменения атрибутов безопасности пользователя, ассоциированных с субъектами. Рассматриваемый компонент сопоставлен с целями **O.Discretionary_Access, O.Auditing** и способствует их достижению.

FMT_MOF.1 Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает модификацию и определения режимов выполнения, отключения и подключения ряда функций только уполномоченному администратору. Рассматриваемый компонент сопоставлен с целью **O.Manage** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает ограничение возможности модификации атрибутов управления доступом объектов только определенным, согласно политике дискреционного управления доступа, субъектам. Рассматриваемый компонент сопоставлен с целями **O.Discretionary_Access, O.Manage** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности и возможность для создателя объекта определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **O.Discretionary_Access, O.Manage** и способствует их достижению.

FMT_MTD.1 (1) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность удаления очистки и создания журнала аудита только уполномоченным администраторам. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FMT_MTD.1 (2) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность модификации и просмотра контролируемых событий аудита только уполномоченным администраторам. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FMT_MTD.1 (3) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность модификации и инициализации атрибутов безопасности пользователей, кроме аутентификационных данных, только уполномоченным администраторам. Рассматриваемый компонент сопоставлен с целями **O.Manage, O.Protect** и способствует их достижению.

FMT_MTD.1 (4) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность инициализации аутентификационных данных только уполномоченным администраторам. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_MTD.1 (5) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность модификации аутентификационных данных только уполномоченным администраторам и пользователям. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_MTD.2 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность определения ограничений для порогового значения количества неуспешных попыток аутентификации только уполномоченным администраторам. Также определяются действия в случае превышения установленного порогового значения, сводящиеся к блокированию учетной записи пользователя на время, установленное администратором. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента обеспечивает ограничение на возможность отмены атрибутов безопасности, ассоциированных с пользователями в пределах ОДФ только уполномоченным администраторам. Также реализовываются правила немедленной отмены имеющих отношения к безопасности полномочий. Рассматриваемый компонент сопоставлен с целями **O.Manage, O.Limit_Authorization** и способствует их достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента обеспечивает ограничение на возможность отмены атрибутов безопасности, ассоциированных с объектами в пределах ОДФ только уполномоченным пользователям. Также реализовываются правила по правам доступа. Рассматриваемый компонент сопоставлен с целью **O.Discretionary_Access** и способствует ее достижению.

FMT_SAE.1 Ограниченная по времени авторизация

Выполнение требований данного компонента обеспечивает ограничение на возможность назначать срок действия для аутентификационных данных только уполномоченным администраторам.. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_SMR.1 Роли безопасности

Данный компонент включен в ПЗ, вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту определенной роли. Рассматриваемый компонент сопоставлен с целями **O.Manage, O.Limit_Authorization** и способствует их достижению.

FMT_SMR.3 Принятие ролей

Выполнение требований данного компонента обеспечивает требование точного запроса для принятия роли уполномоченного администратора. Рассматриваемый компонент сопоставлен с целью **O.Manage** и способствует ее достижению.

FPT_AMT.1 Тестирование абстрактной машины

Выполнение требований данного компонента обеспечивает тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной. Рассматриваемый компонент сопоставлен с целью **O.Protect** и способствует ее достижению.

FPT_RVM.1 Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **O.Enforcement** и способствует ее достижению.

FPT_SEP.1 Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целями **O.Enforcement, O.Protect** и способствует их достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ПЗ, для того, чтобы учесть зависимости выполнения требований компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени и для учета зависимости выполнения требований компонента FMT_SAE.1 от наличия времени для определения срока действия аутентификационных данных. Рассматриваемый компонент сопоставлен с целью **O.Auditing** и способствует ее достижению.

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

Выполнение требований данного компонента обеспечивает блокирование сеанса пользователя после истечения интервала времени бездействия. Определяются действия, необходимые для разблокирования. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FTA_TSE.1 Открытие сеанса с ОО

Выполнение требований данного компонента обеспечивает возможность отказа в открытии сеанса, основываясь на истечении срока действия аутентификационных данных и на времени доступа в ОО. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FTP_TRP.1 Доверенный маршрут

Выполнение требований данного компонента обеспечивает установление доверенной связи между ФБО и пользователями для целей начальной аутентификации и разблокирования сеанса. Рассматриваемый компонент сопоставлен с целью **O.Trusted_Path** и способствует ее достижению.

6.2.2 Логическое обоснование требований доверия

Требования доверия настоящего ПЗ соответствуют ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности).

Выбор ОУД1 в качестве основы требований доверия в настоящем ПЗ является достаточным для определения допустимости использования ОО, соответствующего настоящему ПЗ, при обработке конфиденциальной информации.

6.2.3 Логическое обоснование зависимостей требований

В таблице 6.4. представлены зависимости функциональных требований.

Таблица 6.4 – Зависимости функциональных требований.

	FAU_GEN.1	**FAU_SAR.1**	**FAU_STG.1**	**FDP_ACC.1**	**FDP_ACF.1**	**FIA_ATD.1**	**FIA_UAU.1**	**FIA_UID.1**	**FMT_MSA.1**	**FMT_MSA.3**	**FMT_MTD.1**	**FMT_SMR.1**	**FPT_STM.1**
FAU_GEN.1													**X**
FAU_GEN.2	**X**							**X**					
FAU_SAR.1	**X**												
FAU_SAR.2		**X**											
FAU_SAR.3		**X**											
FAU_SEL.1	**X**										**X**		
FAU_STG.1	**X**												
FAU_STG.3			**X**										
FAU_STG.4			**X**										
FDP_ACC.1					**X**								
FDP_ACF.1				**X**						**X**			
FDP_RIP.2	**отсутствуют**												
FIA_AFL.1							**X**						
FIA_ATD.1	**отсутствуют**												
FIA_SOS.1	**отсутствуют**												
FIA_UAU.2								**X**					
FIA_UAU.7							**X**						
FIA_UID.2	**отсутствуют**												
FIA_USB.1						**X**							
FMT_MOF.1												**X**	
FMT_MSA.1				**X**								**X**	
FMT_MSA.3									**X**			**X**	
FMT_MTD.1 (1)												**X**	
FMT_MTD.1 (2)												**X**	
FMT_MTD.1 (3)												**X**	
FMT_MTD.1 (4)												**X**	

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_STM.1
FMT_MTD.1 (5)												**X**	
FMT_MTD.2											**X**	**X**	
FMT_REV.1 (1)												**X**	
FMT_REV.1 (2)												**X**	
FMT_SAE.1												**X**	**X**
FMT_SMR.1								**X**					
FMT_SMR.3												**X**	
FPT_AMT.1	**отсутствуют**												
FPT_RVM.1	**отсутствуют**												
FPT_SEP.1	**отсутствуют**												
FPT_STM.1	**отсутствуют**												
FTA_SSL.1							**X**						
FTA_TSE.1	**отсутствуют**												
FTP_TRP.1	**отсутствуют**												

Включение в ПЗ компонентов FAU_GEN.2, FIA_UAU.2 и FMT_SMR.1 требует для удовлетворения зависимостей включения компонента FIA_UID.1. В связи с тем, что в ПЗ включен иерархичный компонент FIA_UID.2 включение компонента FIA_UID.1 не предусмотрено.

Включение в ПЗ компонентов FIA_AFL.1, FIA_UAU.7 и FTA_SSL.1 требует для удовлетворения зависимостей включения компонента FIA_UAU.1. В связи с тем, что в ПЗ включен иерархичный компонент FIA_UAU.2 включение компонента FIA_UAU.1 не предусмотрено.

Включение в ПЗ компонента FMT_MSA.1 требует для удовлетворения зависимости включения компонентов FDP_ACC.1 или FDP_IFC.1. В связи с особенностью функционирования ОО данная зависимость удовлетворена компонентом FDP_ACC.1.

Таким образом, все зависимости включенных в ПЗ функциональных требований были удовлетворены.

6.3 Логическое обоснование требований к стойкости функций безопасности

Термин «стойкость функции» определен в части 1 ОК как характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного режима при прямой атаке на лежащие в ее основе механизмы безопасности. В части 1 ОК определено три уровня стойкости функции: базовая СФБ, средняя СФБ и высокая СФБ. В настоящем ПЗ выбран уровень стойкости функции – средняя СФБ. Средняя СФБ – это уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения. Выбор средней СФБ в качестве минимального уровня стойкости функций безопасности является достаточным для определения допустимости использования ОО, соответствующего настоящему ПЗ, при обработке конфиденциальной информации.