СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Начальник управления ФСТЭК России	Генеральный директор ООО «Майкрософт Рус»
В. Селин	Б.Стеен
« »_____ 2008 года	« »_____ 2008 года

Операционная система Windows® Vista™ с Service Pack 1

Задание по безопасности

MS.Win_Vista_SP1.ЗБ

Версия 1.0

2008

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	– база данных
ЗБ	– задание по безопасности
ИТ	– информационная технология
МЭ	– межсетевой экран
ОДФ	– область действия функции безопасности объекта оценки
ОК	– Общие критерии
ОО	– объект оценки
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
ПФБ	– политика функции безопасности
СФБ	– стойкость функции безопасности
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональное требование безопасности

1 Введение ЗБ

Данный раздел содержит информацию общего характера. Подраздел «Идентификация ЗБ» предоставляет маркировку и описательную информацию, которые необходимы, чтобы контролировать и идентифицировать ЗБ и ОО, к которому оно относится. Подраздел «Аннотация ЗБ» содержит общую характеристику ЗБ, позволяющую определить применимость ОО, к которому относится настоящее ЗБ, в конкретной ситуации. В подразделе «Соглашения» дается описание операций конкретизации компонентов требований безопасности ИТ. В подразделе «Термины и определения» представлены определения основных терминов, специфичных для данного ЗБ. В подразделе «Организация ЗБ» дается пояснение организации документа.

1.1 Идентификация ЗБ

Название ЗБ:	Операционная система Windows Vista с Service Pack 1 с Service Pack 1. Задание по безопасности.
Версия ЗБ:	Версия 1.0.
Обозначение ЗБ:	MS.Win_Vista_SP1.ЗБ.
Идентификация ОО:	Операционная система Windows Vista с Service Pack 1.
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, задание по безопасности, ОУД1, Microsoft®.

1.2 Аннотация ЗБ

Настоящее ЗБ определяет требования безопасности для операционной системы Windows Vista с Service Pack 1.

Объект оценки – клиентская многозадачная и многопользовательская операционная система, обеспечивающая контролируемый доступа субъектов к объектам доступа и располагающая возможностями по управлению используемыми аппаратными средствами.

1.3 Соответствие ОК

Объект оценки и ЗБ согласованы со следующими спецификациями:

- ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003» (**соответствие ПЗ - ОО соответствует всем частям данного ПЗ)**;
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002 (**соответствие части 2 ОК** – ОО соответствует функциональным требованиям, основанным на функциональных компонентах из части 2 ОК);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002 (**усиление части 3 ОК** – требования доверия представлены в виде ОУД1 и, кроме того, включают компонент AVA_SOF.1 из части 3 ОК).

1.4 Соглашения

Руководящий документ Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – Общие критерии) допускает выполнение определенных в части 2 ОК операций над функциональными требованиями. Соответственно в настоящем ЗБ используются операции «уточнение», «выбор», «назначение» и «итерация».

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

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

Операция **«назначение»** используется для присвоения конкретного значения ранее неконкретизированному параметру. Операция **«назначение»** обозначается заключением значения параметра в квадратные скобки, [назначаемое значение].

Операция **«итерация»** используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении разрешенных операций («уточнение», «выбор», «назначение»). Выполнение операции «итерация» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

1.5 Термины и определения

В настоящем ЗБ применяются следующие термины с соответствующими определениями.

Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора.

Аутентификация – процесс установления подлинности информации, предъявленной администратором ОО и пользователем ОО при регистрации.

Достоверность – свойство безопасности активов, обеспечивающее соответствие предусмотренным значениям.

Зависимость – соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть удовлетворено, чтобы и другие требования могли отвечать своим целям.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО (в данном случае – ОС Windows Vista с Service Pack 1).

Идентификатор – уникальный признак администратора ОО или пользователя ОО, однозначно его идентифицирующий.

Конфиденциальность – свойство безопасности активов предотвращать возможность доступа к информации и/или ее раскрытия неуполномоченным лицам, объектам или процессам.

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

Объект оценки – подлежащая оценке ОС Windows Vista с Service Pack 1 с руководствами по эксплуатации.

Политика безопасности ОО – совокупность правил, регулирующих управление, защиту и распределение активов, контролируемых ОО.

Политика функции безопасности – политика безопасности, осуществляемая ФБ.

Продукт ИТ – совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы (в данном случае продукт ИТ совпадает с ОО, идентифицированным в настоящем ЗБ).

Профиль защиты – независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

Ресурс ОО – все, что может использоваться или потребляться в ОО (вычислительные возможности, физическая память, дисковое пространство).

Система ИТ – специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Субъект ОО (субъект доступа) – сущность в пределах ОДФ, которая инициирует выполнение операций.

Функции безопасности ОО – совокупность всех функций безопасности ОО, направленных на осуществление ПБО.

Целостность – свойство безопасности активов, обеспечивающее поддержание полноты и неизменности информации.

1.6 Организация ЗБ

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

Раздел 2 «Описание ОО» содержит описание функциональных возможностей ОО, среды функционирования ОО и границ ОО, служащее цели лучшего понимания 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 требования доверия к безопасности ОО.

В раздел 6 «Краткая спецификация ОО» включено описание реализуемых ОО функций безопасности ИТ, соответствующих специфицированным в ЗБ функциональным требованиям безопасности, а также мер доверия к безопасности, соответствующих специфицированным в ЗБ требованиям доверия к безопасности ОО.

В разделе 7 «Утверждения о соответствии ПЗ» идентифицируется ПЗ, о соответствии которому заявляется в ЗБ, а также дополнения и уточнения аспектов среды безопасности, целей и требований безопасности.

В Разделе 8 «Обоснование» демонстрируется, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает

идентифицированные аспекты среды безопасности ИТ, а также что функции безопасности ИТ и меры доверия к безопасности соответствуют требованиям безопасности ОО.

2. Описание ОО

Объектом оценки является операционная система Windows Vista с Service Pack 1 следующих выпусков:

- Windows Vista Business;
- Windows Vista Enterprise;
- Windows Vista Ultimate.

Выпуск Business является базовым для распространения на предприятиях и содержит ряд функций, ориентированных для использования в бизнес-среде. Выпуск Enterprise распространяется только среди корпоративных партнеров компании Microsoft. В дополнение к выпуску Business он содержит следующие функциональные возможности: поддержка всех языков интерфейса, лицензии на 4 виртуальные операционные системы, подсистема поддержки UNIX-приложений. Выпуск Ultimate содержит все функциональные возможности всех выпусков.

Каждый выпуск Windows Vista с Service Pack 1 имеет две версии: для установки на 32-битные системы и 64-битные системы. На системы с 64-битным процессором возможна установка как 32- , так и 64-битных вариантов ОС.

Основные отличия 64-битных версий от 32-битных в следующем:

- отсутствует ограничение объема оперативной памяти в 4 Гбайта;
- защита ядра системы и запрет установки неподписанных драйверов;
- нельзя устанавливать 32-битные драйвера устройств и запускать 16-битные программы.

2.1 Тип продукта ИТ

Операционная система Windows Vista с Service Pack 1 – клиентская многозадачная и многопользовательская операционная система. Операционная система Windows Vista с Service Pack 1 предоставляет надежную инфраструктурную платформу для поддержки одноранговых и клиент-серверных вычислительных сетей, стека протоколов TCP/IP нового поколения, поддерживающего двухуровневую архитектуру IP, в которой протоколы IPv4 и IPv6 совместно используют общий транспортный уровень. Протоколы IPv4 и IPv6 включены по умолчанию, для IPv6 не нужно устанавливать отдельные компоненты. Стек TCP/IP нового поколения автоматически определяет

сетевую среду и настраивает основные параметры, такие как окно приема TCP. В операционной системе Windows Vista с Service Pack 1 реализована собственная архитектура беспроводных сетей Native WiFi.

В состав Windows Vista с Service Pack 1 включен сервер IIS (Internet Information Server v.7.0), предоставляющий платформу для размещения веб-узлов в вычислительных сетях.

Операционная система Wndows Vista располагает возможностями по управлению используемыми аппаратными и вычислительными ресурсами, такими как процессорное время, оперативная память, устройства ввода-вывода и др.

Операционная система Windows Vista с Service Pack 1 располагает интуитивно понятным пользовательским интерфейсом Windows Aero, графическое оборудование которого поддерживает технологию WDDM(Windows Display Driver Model), средствами управления электропитанием и поддерживает технологию UPnP (Universal Plug and Play), позволяющую устранить ручное конфигурирование и обеспечить автоматическое обнаружение различных устройств.

Операционная система Windows Vista с Service Pack 1 характеризуется как управляемая, надежная и безопасная система. Эти свойства ОС достигаются за счет использования файловой системы NTFS, защитника Windows (Windows Defender), обеспечивающего обнаружение, удаление и блокирование шпионских и других нежелательных программ в режиме реального времени, межсетевого экрана Windows Firewall, поддерживающего фильтрацию входящего и исходящего трафика, Internet Explorer 7 в защищенном режиме, единого входа в систему, безопасного хранения реквизитов пользователя и др.

2.2 Основные функциональные возможности операционной системы Windows Vista с Service Pack 1

В Windows Vista с Service Pack 1 реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность, надежность, упрощенное администрирование и управление вычислительной средой ОС. В данном подразделе представлено краткое описание этих функциональных возможностей и средств.

2.2.1 Основные функциональные возможности обеспечения безопасности

В ОС Windows Vista с Service Pack 1 включены средства, позволяющие защитить выбранные файлы, приложения и ресурсы. В число таких средств входят списки управления доступом ACL (Access Control Lists), группы безопасности и групповая политика, средство контроля учетных записей пользователей (User Account Control, UAC), защитник Windows (Windows Defender), а также инструменты, позволяющие настраивать эти средства и управлять ими. Вместе они обеспечивают мощную и гибкую инфраструктуру управления доступом.

2.2.1.1 Групповая политика

Для редактирования параметров групповой политики локального компьютера служит Редактор объектов групповой политики.

2.2.1.2 Защитник Windows

В состав Windows Vista с Service Pack 1 входит Защитник Windows (Windows Defender), который обнаруживает, удаляет или блокирует шпионские и другие нежелательные программы в режиме реального времени. Защитник Windows содержит 9 агентов безопасности, которые постоянно наблюдают за теми критическими областями Windows Vista с Service Pack 1, которые наиболее подвержены изменениям со стороны вредоносных программ. К таким областям относятся:

- программы, автоматически запускаемые при загрузке Windows Vista с Service Pack 1;
- параметры настройки безопасности Windows Vista с Service Pack 1;
- приложения, загружаемые совместно с браузером;
- настройки безопасности браузера;
- файлы и приложения, предназначенные для работы с Internet Explorer (например, ActiveX controls);
- службы и драйвера;
- выполняемые приложения;
- инструменты и файлы Windows Vista с Service Pack 1, используемые для регистрации запускаемых приложений;
- программные утилиты Windows Vista с Service Pack 1.

Если в результате проверки Защитник Windows, запущенный вручную, обнаруживает опасные объекты, то пользователю выдается предупреждение и предлагается выбрать следующие действия:

- удалить объект;
- переместить объект в карантин;
- разрешить выполнение объекта и поместить его в список разрешенных;
- игнорировать предупреждение.

При обнаружении опасных объектов в автоматическом режиме проверки Защитник Windows выполняет действия в зависимости от установленных настроек.

2.2.1.3 Группы безопасности

Группы безопасности позволяют упростить управление доступом к активам, позволяя назначать разрешения на доступ группе пользователей, а не отдельной учетной записи. Таким образом, исходя из потребностей в доступе к новым активам, учетная запись может быть просто добавлена или удалена из группы.

Кроме пользователей в группу безопасности можно добавлять компьютеры и другие группы безопасности. Добавляя компьютеры в группу безопасности, можно упростить предоставление доступа системной задачи одного компьютера к активам другого.

После установки в ОС Windows Vista с Service Pack 1 по умолчанию создаются встроенные группы, дающие право выполнять предопределенные системные задачи. Исходя из модели построения сети – модель рабочей группы (workgroup) или доменная модель (domain)– встроенные группы подразделяются на:

- встроенные локальные группы безопасности (built-in local group);
- встроенные доменные локальные группы безопасности (built-in domain local group);
- встроенные глобальные группы безопасности (built-in global group).

2.2.1.4 Списки управления доступом

В ОС Windows Vista с Service Pack 1 доступ к активам системы разрешен только уполномоченным на это пользователям. Модель защиты ОС Windows Vista с Service Pack 1 включает компоненты, которые реализуют контроль субъектов доступа, действий,

предпринимаемых конкретной сущностью по отношению к объекту доступа и аудит событий.

Каждый объект доступа, представленный в ОС Windows Vista с Service Pack 1, однозначно ассоциирован с дескриптором безопасности, главными компонентами которого являются: дискреционный список контроля доступа, который определяет права доступа к объекту и системный список контроля доступа, служащий для определения параметров аудита. Дискреционный список контроля доступа включает перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

2.2.1.5 Средство контроля учетных записей

Для предотвращения несанкционированного доступа к ресурсам в Windows Vista с Service Pack 1 реализовано средство контроля учетных записей пользователей – User Account Control (UAC), которое обеспечивает:

- пересмотр операций, которые ранее требовали административных прав (например, устанавливать критические обновления Windows);
- облегченную виртуализацию, которая помогает программам правильно работать без административных привилегий;
- возможность явного запроса программами административных прав ;
- изоляцию административных процессов от неадминистративных, работающих в той же пользовательской среде.

В Windows Vista с Service Pack 1 все учетные записи, относящиеся к группе «Администраторы», по умолчанию работают с правами обычного пользователя. Если пользователь или приложение пытается выполнить действие, для которого требуются полномочия администратора, появляется окно UAC с требованием подтвердить или отменить выбранную команду. После подтверждения запроса система временно повышает права пользователя до уровня администратора.

2.2.1.6 Аудит событий безопасности

Операционная система Windows Vista с Service Pack 1 располагает достаточным набором средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, и событий, которые могут произойти в вычислительной среде.

ОС позволяет получать копии событий, зарегистрированных на различных удаленных компьютерах, и сохранять их локально. Для этого необходимо создать подписку на события, включающую перечень получаемых данных и журнал для их хранения на локальном компьютере. За процесс передачи и сбора информации отвечают служба удаленного управления Windows (WinRM) и служба сбора событий Windows (Wecsvc). Обе службы должны быть запущены на компьютерах, участвующих в процессе передачи и сбора событий.

Мониторинг системных событий позволяет обнаруживать нарушителей системы безопасности, а также выявлять попытки фальсифицировать данные, находящиеся на локальном компьютере. При аудите чаще всего встречаются такие события как доступ к объектам, управление группами безопасности и учетными записями пользователей, а также вход пользователей в систему и выход из нее. В частности, аудит позволяет вести мониторинг конкретных событий, например, неудачных попыток входа в систему. Просмотр журнала безопасности выполняется с помощью средства просмотра событий. Политика аудита позволяет определять, для каких категорий событий должен проводиться аудит.

2.2.1.7 Принудительное применение учетной записи гостя

Модель общего доступа и безопасности для локальных учетных записей позволяет выбирать между моделью «только гость» (Guest only) и классической моделью безопасности (Classic). В модели «только гость» доступ к компьютеру из сети может быть осуществлен только с учетной записью гостя. В гостевой модели все пользователи считаются равноправными. В классической модели безопасности пользователи, пытающиеся получить доступ к локальному компьютеру из сети, идентифицируются под своими учетными записями.

Если существует учетная запись гостя с пустым паролем, она разрешает вход в систему и доступ к любым ресурсам, на которые предоставляет полномочия эта учетная запись.

Если действует политика «принудительное назначение прав гостя при входе с локальной учетной записью» (force network logons using local accounts to authenticate as Guest), локальная учетная запись должна идентифицироваться как «гость». Эта политика определяет, следует ли обязательно идентифицировать пользователя, который устанавливает подключение из сети непосредственно к компьютеру, как гостя. Таким

образом, ограничиваются разрешения, предоставляемые локальным пользователям, пытающимся получить доступ к активам компьютера. Если эта политика включена, всем локальным пользователям, пытающимся непосредственно подключиться к компьютеру, предоставляется уровень разрешений гостя, который, как правило, существенно ограничен и не позволяет изменять системные настройки и получать доступ к файлам других пользователей.

2.2.1.8 Ограничения на пустой пароль

Чтобы обеспечить защиту активов в случаях использования пустого пароля, в ОС Windows Vista с Service Pack 1 учетные записи, не имеющие пароля, могут быть использованы только для доступа с локальной консоли компьютера. По умолчанию запрещается применять учетные записи с пустым паролем. В частности, нельзя применять в качестве локального пользователя с пустым паролем службу вторичного доступа в систему (службу RunAs) для запуска программ.

Присвоение пароля локальной учетной записи снимает ограничения на доступ в систему через сеть. Кроме того, при этом разрешается доступ с данной учетной записью к любым активам, на которые распространяются связанные с ней полномочия, в том числе и через подключение по сети.

2.2.1.9 Управление учетными данными

Функция управления учетными данными обеспечивает безопасное хранение учетных данных пользователя, включая пароли и сертификаты X.509. Пользователям предоставляется возможность согласованной однократной регистрации. Если пользователю необходимо получить доступ к приложению в сети, то при осуществлении его первой попытки потребуется выполнить проверку подлинности, в ходе которой пользователю будет предложено ввести свои учетные данные. После ввода эти данные связываются с запрошенным приложением. При осуществлении в будущем попыток доступа к этому приложению сохраненные учетные данные будут использоваться повторно.

2.2.1.10 Хранение имен пользователей и паролей

Хранение имен пользователей и паролей осуществляется в безопасном перемещаемом хранилище. Доступ к учетным данным регулируется параметрами локальной безопасности LSS (Local Security Settings).

2.2.2 Основные функциональные возможности повышения надежности

2.2.2.1 Защита файлов Windows

Средства защиты файлов Windows работают в фоновом режиме и предотвращают возможность изменения или замещения системных файлов другими программами. Данный механизм позволяет исключить вероятность аварийного завершения работы системы или отказа приложений в случаях модификации, перемещения или удаления системных файлов, произошедших по неосторожности или в результате воздействия системных вирусов и других вредоносных программ.

Механизм работы подсистемы WFP основан на проверке наличия цифровой подписи в файле, которая удостоверяет, что данный файл прошел соответствующую проверку и не был изменен или заменен в процессе установки каких-либо других программ. Если подпись отсутствует или неправильна, поверх модифицированного файла будет записана его исходная версия, извлеченная из папки dllcache.

В зависимости от параметров, заданных администратором при настройке компьютера, ОС Windows Vista с Service Pack 1 либо игнорирует драйверы устройств, не имеющие цифровой подписи, либо предупреждает об обнаруженных драйверах без цифровой подписи (этот режим принимается по умолчанию), либо запрещает установку неподписанных драйверов.

2.2.2.2 Мониторинг завершения работы

Операционная система Windows Vista с Service Pack 1 содержит утилиту мониторинга завершения работы (Shutdown Event Tracker), использующую механизм детального документирования причин отключения и перезапуска компьютера. Эти данные используются для анализа причин аварийного завершения работы компьютера и более полного анализа системной среды.

Кроме документирования причин завершения работы, утилита Shutdown Event Tracker также осуществляет «моментальный снимок» состояния системы перед отключением, определяет, какие системные ресурсы были перегружены или близки к

перегрузке. Она также регистрирует ряд параметров всех процессов в системе, страничных файлов, дисков и общие сведения об использовании системных ресурсов.

2.2.2.3 Архивация данных

В ОС Windows Vista с Service Pack 1 входят программа архивации и системные средства, предоставляющие пользователям возможность выполнять архивирование файлов и папок на несъемные и съемные устройства хранения (компакт-диск или DVD). Одним из эффективных вариантов применения этих средств архивации является настройка их для регулярной архивации локальных файлов на сервер, данные с которого впоследствии архивируются в соответствии с порядком, принятым в организации.

Для управления архивацией в ОС Windows Vista с Service Pack 1 имеется оснастка Центр архивации и восстановления. Он позволяет автоматизировать выполнение архивации, создать полный архив состояния компьютера (архивный образ Complete PC) и восстановить данные из созданных архивов.

2.2.2.4 Теневое копирование тома

Служба теневого копирования тома управляет созданием теневых копий (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления или для иных целей. Служба теневого копирования тома обеспечивает копирование данных в реальном режиме времени, не теряя их согласованности и не прерываясь в случаях открытия файлов в момент копирования.

2.2.2.5 Откат драйверов

Данная возможность способствует обеспечению устойчивости ОС Windows Vista с Service Pack 1. При обновлении драйвера копия предыдущего пакета драйверов автоматически сохраняется в специальном подкаталоге системных файлов (для каждого архивируемого драйвера добавляется новое значение к ключам архивации, размещенным в соответствующем разделе реестра). Если новый драйвер будет работать неудовлетворительно, пользователь может восстановить предыдущую версию драйвера, перейдя в «Диспетчере устройств» на вкладку «Драйвер» (Driver) для соответствующего устройства и нажав кнопку «Откатить» (Roll Back Driver). Откат драйвера разрешается производить на один предшествующий уровень, поскольку только одна версия

предыдущего драйвера может сохраняться при выполнении обновления. Данная возможность доступна для всех классов устройств, за исключением принтеров.

2.2.2.6 Восстановление системы

Функциональная возможность восстановления системы позволяет возвращать компьютер в то состояние, в котором он находился до возникновения проблемы. При этом не происходит потери личных файлов данных, которые могут содержать, например, документы, изображения или сообщения электронной почты. При использовании данной возможности осуществляется активный мониторинг изменений системных характеристик и некоторых файлов приложений, а также автоматическое создание легко идентифицируемых контрольных точек восстановления. В ОС Windows Vista с Service Pack 1 создание контрольных точек восстановления производится по умолчанию каждый день, а также при значительных изменениях характеристик системы, таких, например, как установка приложения или драйвера. Пользователь также имеет возможность в любое время самостоятельно создать собственные контрольные точки восстановления. При использовании функции восстановления системы мониторинг изменений и восстановление файлов с личными данными не производится.

2.2.2.7 Аварийное восстановление системы

Функция аварийного восстановления системы ASR (Automated System Recovery) обеспечивает возможность восстановления системы в случае серьезного повреждения системы или сбоя/замены жесткого диска. ASR архивирует состояние системы, системные службы и все диски, связанные с компонентами операционной системы. Кроме того, с ее помощью создается загрузочный диск, содержащий сведения об архивации, конфигурациях диска (включая базовый и динамический тома) и инструкции по выполнению восстановления.

Совместное использование ASR и стандартных механизмов архивации позволяет обеспечить восстановление системы до исходного состояния, предшествовавшего сбою. Применение этой функциональной возможности целесообразно в различных сценариях восстановления системы после возникновения аварийной ситуации; например, в случае сбоя жесткого диска и потери всех конфигурационных параметров и информации.

2.2.3 Основные средства администрирования, управления и поддержки

2.2.3.1 Использование дисковых квот

Механизм дисковых квот позволяет отслеживать и контролировать использование пользователями места на диске для томов NTFS. Администраторы могут настроить ОС Windows Vista с Service Pack 1 таким образом, чтобы:

- запретить использование дискового пространства сверх указанного предела и регистрировать случаи превышения этого предела пользователями;
- регистрировать события превышения пользователями указанного порога предупреждения, то есть отметки, при прохождении которой пользователь приближается к заданному для него пределу использования дискового пространства.

Дисковые квоты основаны на владении файлами и не зависят от расположения файла или папки пользователя на томе. Дисковые квоты применяются только к томам и не зависят ни от структуры папок на томах, ни от схемы размещения томов на физических дисках. Если один физический диск содержит несколько томов и квоты применяются к каждому тому, то каждая квота применяется только к указанному тому. Квоты можно включать на локальных томах, сетевых томах и съемных дисках с файловой системой NTFS.

2.2.3.2 Инструментарий управления Windows

Инструментарий управления Windows (Windows Management Instrumentation) представляет собой реализацию компанией Microsoft протокола WBEM (Web-Based Enterprise Management – управление предприятием на основе веб-технологий), регламентирующего стандарты общего доступа к данным управления по сети предприятия. WMI обеспечивает встроенную поддержку модели CIM (Common Information Model – общая модель данных), которой должны соответствовать объекты среды управления.

WMI включает CIM-совместимую базу данных, в которой хранятся определения объектов, и диспетчер объектов CIM, в задачи которого входит занесение объектов в хранилище и управление ими, а также сбор данных от поставщиков WMI. Поставщики WMI играют роль посредников между WMI и компонентами операционной системы, приложениями и другими системами. Например, поставщик реестра получает данные из реестра, а поставщик SNMP предоставляет данные и события от устройств SNMP.

Поставщики не только предоставляют данные, но и методы, с помощью которых можно управлять компонентами, свойства, которые могут быть изменены, и события, информирующие об изменениях, происходящих в компонентах.

WMI может использоваться средствами управления компьютерами, такими как Microsoft Systems Management Server. Кроме того, WMI применяется в других технологиях, таких как Microsoft Health Monitor и Microsoft Operations Manager, а также сторонними изготовителями компьютерных систем управления. Можно также использовать WMI вместе с системами программирования (такими как Windows Script Host) как для получения сведений о конфигурации компьютерных систем, в том числе о серверных приложениях, так и для изменения конфигурации.

2.2.3.3 Консоль управления MMC

Консоль управления Microsoft Management Console (MMC) – средство для создания, сохранения и открытия средств администрирования (называемых оснастками MMC), с помощью которых осуществляется управление оборудованием, программными и сетевыми компонентами ОС Windows Vista с Service Pack 1.

2.2.3.4 Средства администрирования

В составе ОС Windows Vista с Service Pack 1 интегрированы следующие средства администрирования:

- **управление компьютером** – используется для управления локальными или удаленными компьютерами. Оснастка «Управление компьютером» объединяет несколько средств администрирования ОС Windows Vista с Service Pack 1 в одно дерево консоли, что обеспечивает легкий доступ к свойствам администрирования конкретного компьютера;
- **источники данных (ODBC)** – ODBC (Open Database Connectivity) – программный интерфейс, с помощью которого программы получают доступ к данным в системах управления базами данных, использующих язык SQL как стандарт доступа к данным;
- **просмотр событий** – используется для просмотра и управления журналами системных и программных событий, а также событий безопасности на компьютере. В окне просмотра событий отображаются сведения о неисправностях оборудования и сбоях программного обеспечения, а также

отображаются события безопасности. Имеется возможность отбирать события из нескольких журналов по различным критериям, настройки автоматического запуска программ при возникновении определенного события, а так же получения сведений о событиях с удаленных компьютеров;

- **монитор** производительности и стабильности – предоставляет средства анализа производительности системы. С помощью одной консоли пользователь может в реальном времени осуществлять контроль производительности приложений и оборудования, задавать пороговые данные для оповещений и автоматических действий, генерировать отчеты и просматривать историю производительности системы, используя различные способы сортировки.
- **службы** – используются для управления службами компьютера, установки действий по восстановлению в случае сбоя службы и создания пользовательских имен и описаний служб для упрощения их определения;
- **локальная политика безопасности –** используется для настройки параметров безопасности локального компьютера. Такими параметрами помимо прочих, являются политика паролей, политика учетных записей, политики аудита, политика безопасности IP, определение присвоения прав пользователям. Локальная политика безопасности доступна только на компьютерах, которые не являются контроллерами домена. Если компьютер является членом домена, эти параметры могут быть переопределены в политиках, полученных из домена;
- **управление печатью** – предоставляет единый интерфейс эффективного администрирования нескольких принтеров и серверов печати;
- **брандмауэр Windows в режиме повышенной безопасности** – объединяет брандмауэр компьютера и IPsec. Обеспечивает локальную защиту от сетевых атак через локальную сеть, безопасность межкомпьютерного подключения и проверку подлинности и защиту данных при взаимодействии;
- **планировщик заданий** – позволяет назначить автоматически выполняемые задания, запуск которых производится в определенное время или при возникновении определенных событий. Планировщик заданий содержит библиотеку всех назначенных заданий, обеспечивая возможность быстрого просмотра и удобного управления заданиями;

- **инициализатор iSCSI** – используется для настройки прямых подключений к запоминающим устройствам в сети
- **конфигурация системы** – средство выявления проблем при загрузке системы;
- **средство диагностики памяти** – обеспечивает проверку памяти компьютера. Выполняется в двух режимах: после перезагрузки системы и при включении компьютера.

2.2.3.5 Результирующий набор политик

Многие параметры политик могут быть изменены в нескольких места: в конфигурации пользователя, конфигурации компьютера. Оснастка «Результирующая политика» позволяет отобрать только измененные параметры политик и определить итоговое значение для конкретного пользователя или компьютера, что является мощным и гибким средством для планирования, мониторинга и устранения ошибок при работе с групповой политикой.

2.2.3.6 Служба терминалов

Служба терминалов (Terminal Services) позволяет компьютерам в локальной сети (LAN) подключаться к удаленным компьютером и запускать находящиеся на нем программы. Она обеспечивает запуск уникальных сеансов пользователей, что позволяет разделить данные различных пользователей. Если применяются пароли пользователей, то сеансы являются взаимно безопасными.

2.2.3.8 Центр безопасности Windows

Центр безопасности Windows сводит в единое целое всю информацию о состоянии безопасности на компьютере и отправляет пользователю специальные сообщения о необходимости обновления приложений, предназначенных для обеспечения безопасности, и наличии в параметрах безопасности потенциально уязвимых мест, которые следует устранить. Так, в центре безопасности WSC может отображаться состояние параметров межсетевого экрана и сведения о том, настроен ли компьютер на автоматический прием обновлений от корпорации Microsoft. Кроме того, этот компонент осуществляет мониторинг приложений для защиты от вирусов и шпионских программ, оповещая пользователя, если такие приложения отсутствуют или требуют обновления.

Проверяются также параметры безопасности Internet Explorer и функции контроля учетных записей пользователей. Если они являются недостаточно надежными, центр безопасности Windows сообщает об этом пользователю и предоставляет рекомендации по устранению проблемы;

2.2.4 Основные функциональные возможности обеспечения сетевой безопасности

2.2.4.1 Контролируемый доступ из сети

Операционная система Windows Vista с Service Pack 1 располагает встроенными средствами безопасности, позволяющими препятствовать несанкционированному вторжению. Это достигается путем ограничения привилегий тех субъектов, которые пытаются получить удаленный доступ к компьютеру, до уровня «гость». Функционирование ОС Windows Vista с Service Pack 1 базируется на ограничении прав любого, кто попытается осуществить доступ к компьютеру и получить несанкционированные привилегии путем подбора паролей, доступ данных субъектов будет либо невозможен, либо субъект получит только ограниченный доступ на уровне «гостя».

Операционная система Windows Vista с Service Pack 1 по умолчанию сопоставляет всех пользователей, осуществляющих удаленный доступ, с учетной записью «гость». Таким образом, предотвращаются попытки злоумышленников получить удаленный доступ к компьютеру посредством локальной учетной записи администратора ОС Windows Vista с Service Pack 1, не имеющей пароля.

2.2.4.2 Брандмауэр сетевых подключений

Операционная система Windows Vista с Service Pack 1 обеспечивает защиту доступа в сети средствами встроенного брандмауэра сетевых подключений (Windows Firewall). Брандмауэр сетевых подключений обеспечивает защиту компьютера с установленной ОС Windows Vista с Service Pack 1, непосредственно подключенного к сети, или персональных компьютеров и устройств, подключенных к компьютеру с установленной ОС Windows Vista с Service Pack 1, через который осуществляется общий доступ к внешним сетям.

В брандмауэре сетевых подключений реализован механизм активной фильтрации пакетов, порты брандмауэра открываются динамически только на время, необходимое для

получения доступа к запрашиваемым услугам. Данная технология противодействует попыткам сканирования портов и ресурсов и прочих активов компьютера, в том числе папок и принтеров с общим доступом. При этом существенно снижается угроза внешних атак.

Брандмауэр, взаимодействуя с технологией ограничения полномочий служб Windows Servise Hardening, позволяет предотвратить использование системных служб Windows для выполнения непредусмотренных действий в файловой системе, системном реестре или сети.

Брандмауэр поддерживает фильтрацию входящего и исходящего трафика, применение сетевых правил ограничения полномочий системных служб, блокирование обмена данными по сети локально функционирующих приложений.

В Windows Vista с Service Pack 1 управление брандмауэром и протоколом IPSec собраны на консоли Брандмауэр Windows в режиме повышенной безопасности (Windows Firewall with Advanced Security). Это позволяет централизованно управлять фильтрацией трафика пакетов и параметрами IPSec

2.2.4.3 Клиент защиты сетевого доступа

Клиент защиты сетевого доступа Network Access Protection (NAP) помогает обеспечить защиту от атак по сети на основе списка требований к состоянию клиентских компьютеров и проверки соблюдения этих требований при подключении компьютера к сети.

2.2.4.4 Поддержка стандартов безопасности

Операционная система Windows Vista с Service Pack 1 обеспечивает возможность поддержки безопасных вычислительных сетей, построенных на основе таких стандартов безопасности как SSL/TSL, IPSec (Internet Protocol Security) и Kerberos.

IP-безопасность интегрирована со стеком TCP/IP и обеспечивает защиту IP-данных от перехвата и несанкционированных манипуляций, а также защиту от сетевых атак различных типов. Использование прокола IPSec позволяет обеспечить безопасность данных, передаваемых по сети. Протокол безопасности IPSec играет важную роль в обеспечении безопасности виртуальных частных сетей (VPN), обеспечивающих возможность безопасной передачи данных через менее доверенные вычислительные сети.

В ОС Windows Vista с Service Pack 1 аутентификационные данные пользователя могут быть представлены в виде пароля, мандата Kerberos или смарт-карты, если компьютер оборудован для работы со смарт-картами.

Протокол аутентификации Kerberos обеспечивает средства взаимной проверки подлинности клиентов, например пользователя, компьютера или службы и сервера. Используя поддержку протокола Kerberos ОС Windows Vista с Service Pack 1 предоставляет пользователям возможность однократного ввода аутентификационных данных для доступа ко всем активам и поддерживаемым приложениям, права на доступ к которым у них имеются.

2.2.4.5 Microsoft Internet Explorer в защищенном режиме

Microsoft Internet Explorer в защищенном режиме обеспечивает защиту пользователей от вредоносных программ и безопасность пользовательских данных посредством запрета записи информации в папку «Мой компьютер», кроме временных файлов Интернета, а также запрета Internet Explorer на внесение изменений в пользовательские и системные файлы.

Для защиты пользовательских данных Internet Explorer содержит:

- фильтр фишинга, формирующий предупреждение пользователю о подозрительных web-узлах, выполняющих несанкционированный сбор конфиденциональной информации;
- строку состояния безопасности, содержащую сведения о безопасности и надежности web-узлов;
- адресную строку во всех окнах, предоставляющую пользователям получить сведения об истинном источнике информации.

2.3 Среда функционирования и границы ОО

2.3.1 Среда функционирования

Возможная среда функционирования ОО определяется конфигурациями Enterprise и High Security.

Enterprise

Среда Enterprise Client (EC) включает домен со службой каталогов Active Directory, в котором компьютеры с ОС Microsoft® Windows® Server 2003 Release 2 или ОС Microsoft® Windows® Server 2003 с пакетом обновления 1 (SP1) управляют клиентскими компьютерами с ОС Windows Vista с Service Pack 1 или ОС Microsoft® Windows® XP. В такой среде управление клиентскими компьютерами осуществляется с помощью групповой политики, которая применяется к сайтам, доменам и подразделениям. Групповая политика обеспечивает централизованную инфраструктуру на базе Active Directory, которая позволяет выполнять изменения на уровне доменов и управлять конфигурацией пользователей и параметрами компьютеров, включая параметры безопасности и данные пользователей.

High Security

Среда **High Security** (HS) позволяет создать среду с повышенной безопасностью для компьютеров под управлением ОС Windows Vista с Service Pack 1. Безопасность этой среды настолько важна, что существенное уменьшение функциональности и возможностей управления считается приемлемой.

2.3.2 Логические границы ОО

Объект оценки – это модульная система, состоящая из программных компонентов, работающих либо в непривилегированном режиме процессора (пользовательском режиме), либо в привилегированном режиме процессора (режиме ядра), и совместно выполняющих разные задачи. Каждый компонент ОО реализует определенные функции, которые служат своеобразным интерфейсом для остальной части системы (см. рисунок 1).

Наличие двух режимов обусловлено необходимостью предотвращения прямого доступа приложений к критически важным данным ОО и устранения риска их модификации. Таким образом, выполнение кода приложений осуществляется в пользовательском режиме, а кода ОО (например, системные сервисы и драйверы устройств) – в режиме ядра, что обеспечивает невозможность нарушения стабильности работы всего ОО в случаях сбоя отдельных приложений. В режиме ядра обеспечивается доступ к системным данным и аппаратным средствам, а также выполнение любых машинных команд процессора.

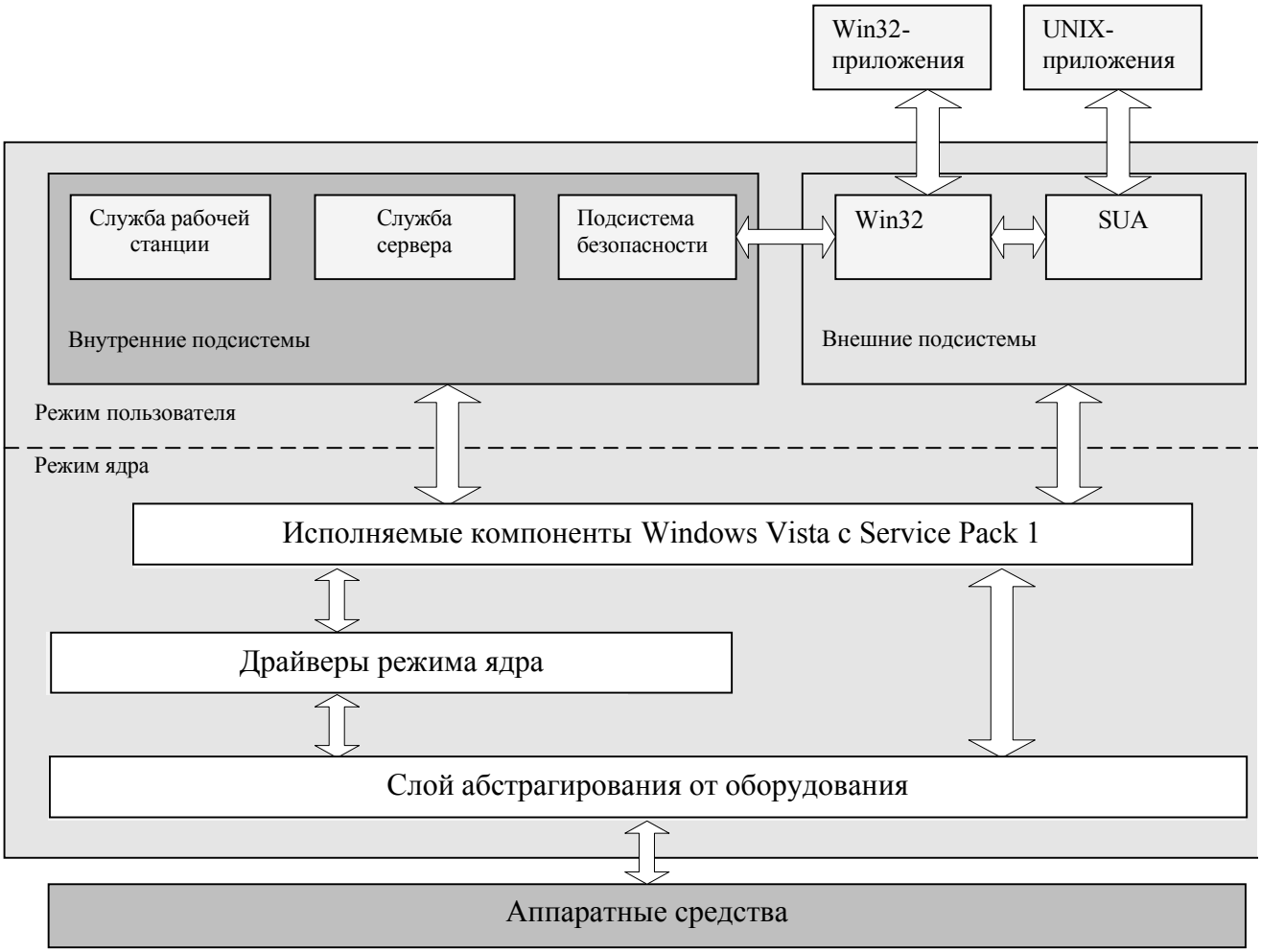

Рисунок 1 – Взаимодействие основных компонентов ОО

2.3.3 Физические границы ОО

Физические границы ОО включают персональный компьютер со следующими характеристиками:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с частотой 1ГГц;
- 1 Гбайт оперативной памяти;
- графический процессор с поддержкой Windows Aero;
- жесткий диск объемом не менее 40 Гбайт с 15 Гбайтами свободного дискового пространства;
- привод DVD;
- сетевой адаптер.

2.4 Службы безопасности ОО

В данном подразделе приводится краткое описание служб безопасности ОО, реализующих оцениваемые (в соответствии с настоящим ЗБ) функции безопасности ОО.

2.4.1 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 ОО и может детализироваться вплоть до доступа к конкретным файлам или каталогам отдельных пользователей или групп. После настройки параметров аудита можно отслеживать доступ пользователей к определенным объектам и анализировать недостатки системы 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.

2.4.2 Защита данных пользователя

Объект оценки осуществляет функции и политику избирательного (дискреционного) управления доступом, фильтрацию информации, а также реализует механизм защиты остаточной информации. Избирательное управление доступом предоставляет возможность ограничивать и контролировать доступ к системе,

приложениям и ресурсам, таким как файлы, папки и принтера. Каждый пользователь, пытающийся получить доступ к системе, сначала проходит процедуру идентификации и аутентификации, а затем, при попытках получения доступа к ресурсам, – авторизацию, т.е. проверку разрешений пользователя по отношению к какому-либо защищаемому объекту. Вся информация, определяющая безопасность защищаемого объекта, хранится в ассоциированном с ним дескрипторе безопасности, который формируется при создании объекта и впоследствии может меняться. Изменять содержимое дескриптора безопасности могут пользователи, имеющие статус владельца объекта, а также субъекты, которым предоставлены соответствующие полномочия. Главными компонентами дескрипторами безопасности объекта являются дискреционный список управления доступом, который собственно и определяет права доступа к объекту, и системный список контроля доступа, служащий для назначения аудита.

Объект оценки обеспечивает фильтрацию входящей в ОО (исходящей из ОО) информации (защиту доступа в сети) с использованием брандмауэра сетевых подключений, а также защиту от вредоносных программ, выявляя, блокируя, и удаляя их в реальном масштабе времени. ОО также обеспечивает защиту данных пользователя посредством механизма, обеспечивающего обезличивание (обнуление) остаточной информации в свободных блоках памяти (оперативной и дисковой) перед их предоставлением каким-либо процессам, выполняющимся в режиме пользователя.

2.4.3 Идентификация и аутентификация

Объект оценки требует, чтобы все пользователи уникально идентифицировались и аутентифицировались при входе в ОО с помощью ввода идентификатора и пароля. Идентификация и аутентификация осуществляются до выполнения субъектом доступа 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 поддерживает локальную базу данных (БД), хранящую информацию об учетных записях пользователей, и обращения к каталогам Active Directory. Каждая учетная запись представлена идентификатором пользователя, однозначно связанным с его идентификатором безопасности – SID (Security Identifier), аутентификационной информацией, информацией о членстве в группах безопасности,

ассоциированными правами и полномочиями (привилегиями). ОО обеспечивает хранение паролей в преобразованном формате. ОО предоставляет средства усиления безопасности паролей через использование механизма политик безопасности, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля. ОО предоставляет механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором ОО или по истечении времени действия, заданного для счетчика блокировки.

2.4.4 Управление безопасностью

Объект оценки включает механизмы управления групповыми политиками. Групповая политика является важным средством обеспечения безопасности ОО и обеспечивает управление конфигурацией безопасности пользователей и компьютеров. Использование групповых политик позволяет обеспечить безопасность среды пользователя, задав соответствующие параметры групповых политик в сочетании с разрешениями NTFS и другими средствами безопасности ОО. Полномочия на управление политиками контролируются посредством механизма управления доступом, членства в административных группах и назначаемых полномочий (привилегий).

2.4.5 Защита ФБО

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) и собственно самих функций безопасности ОО обеспечивает поддержание уверенности администратора ОО в целостности и корректности функционирования функций безопасности ОО.

2.4.6 Использование ресурсов ОО

Объект оценки может ограничивать объем доступного для пользователя дискового пространства посредством использования механизма дисковых квот. Дисковые квоты используются для управления объемом хранимых данных и позволяют распределять

дисковое пространство между пользователями в зависимости от того, владельцами каких папок и файлов они являются. ОО позволяет учитывать дисковые квоты для каждого тома, даже если эти тома расположены на одном и том же жестком диске. По умолчанию только члены группы «Администраторы» (Administrators) могут устанавливать дисковые квоты, определять пороги выдачи предупреждений и пределы квот, как для всех пользователей, так и индивидуально для каждого пользователя. Кроме того, администратор ОО уполномочен определять действия, выполняемые системой при превышении квот пользователями.

Для организации использования процессорного ресурса уполномоченному администратору ОО предоставляется механизм установления приоритетов выполняемым процессам.

2.4.7 Блокирование сеанса

Объект оценки предоставляет возможность пользователю блокировать свой сеанс немедленно или по прошествии заданного интервала времени. Деятельность пользователя постоянно контролируется посредством манипулятора типа «мышь» и клавиатуры. Если в течение заданного интервала времени пользователь бездействует, его сеанс блокируется.

Централизованное управление параметрами блокирования сеанса пользователя осуществляется с использованием механизмов групповой политики.

3. Среда безопасности ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

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

3.1 Предположения безопасности

3.1.1 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.

A.TOEConfig

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

3.1.2 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. Не допускается возможность восстановления системы неуполномоченным пользователем с использованием дистрибутивного носителя, позволяющая получить доступ к командной строке с максимально возможными правами и контроль над защищенными папками и файлами.

A.Manage

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

A.No_Evil_Adm

Персонал, ответственный за выполнение администрирования ОО, должен руководствоваться соответствующей документацией.

3.1.3 Предположения, связанные с физической защитой ОО

A.LocateTOE

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 физической модификации.

3.2 Угрозы

В настоящем ЗБ определены следующие угрозы, которым противостоит 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 ограничения доступа к данным, осуществляемого уполномоченными пользователями.

T.FailureTOE

Нарушение режимов функционирования ОО, а также потеря или искажение данных ФБО и пользовательских данных вследствие сбоев и отказов программного обеспечения и оборудования ОО.

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.

P.FiltrationFlow

Должна осуществляться фильтрация входящих в ОО информационных потоков.

P.Warn

Объект оценки должен предупреждать пользователей относительно ответственности за несанкционированное использование ОО.

P.Sec

Объект оценки должен обеспечивать защиту аутентификационных данных, передаваемых удаленным доверенным системам ИТ.

P.SOFAuth

Должен быть предоставлен механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

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.Rezidual_Information

ФБО должны обеспечивать недоступность информационного содержания освобождаемых ресурсов.

O.Manage

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

O.FiltrationFlow

ОО должен располагать механизмами, осуществляющими фильтрацию входящих/исходящих в/из ОО информационных потоков.

O.SafeRecovery

Должна быть обеспечена возможность безопасного восстановления ОО после сбоев и отказов программного обеспечения и оборудования.

O.SOFAuth

ОО должен обеспечивать механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

O.Enforcement

ФБО должны быть спроектированы и реализованы таким образом, чтобы обеспечить 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 и ресурсов, поддерживая домен для своего функционирования.

O.Trusted_Path

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

O.Legal_Warning

ФБО должны располагать механизмами оповещения пользователя об ответственности за использование ОО до предоставления доступа к ресурсам.

O.Limit_Authorization

ФБО должны предоставлять возможность ограничивать уровень полномочий для каждого пользователя.

O.Sec

ФБО должны располагать механизмами, обеспечивающими защиту передаваемых данных ФБО удаленным доверенным системам ИТ.

4.2 Цели безопасности для среды

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

OE.Install

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

OE.Physical

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

OE.Creden

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

OE.TOEConfig

Должны быть обеспечены установка, конфигурация и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

5. Требования безопасности ИТ

В данном разделе ЗБ представлены требования безопасности ИТ, которым должен удовлетворять ОО и его среда. Функциональные требования безопасности, представленные в настоящем ЗБ, основаны на функциональных компонентах из части 2 ОК. Требования доверия основаны на компонентах требований доверия из части 3 ОК и представлены в настоящем ЗБ в виде оценочного уровня доверия ОУД1, усиленного компонентом доверия AVA_SOF.1 (Оценка стойкости функции безопасности ОО). Функция безопасности «Аутентификация» реализуется механизмом паролей. Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости. В качестве минимального уровня стойкости функции безопасности «Аутентификация» в настоящем ЗБ заявлена **«Средняя СФБ»**.

Другие механизмы (некриптографические), реализуемые в интересах обеспечения безопасности ОО, нельзя отнести к вероятностным и перестановочным механизмам, поэтому заявлений об их стойкости в настоящем ЗБ не делается.

5.1 Требования безопасности для ОО

5.1.1 Функциональные требования безопасности ОО

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

Идентификатор компонента требований	Название компонента требований
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_IFC.1	Ограниченное управление информационными потоками
FDP_IFF.1	Простые атрибуты 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
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1	Связывание пользователь-субъект
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_RCV.1	Ручное восстановление
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_ITC.1	Конфиденциальность экспортируемых данных ФБО
FPT_STM.1	Надежные метки времени

Идентификатор компонента требований	Название компонента требований
FPT_TST.1	Тестирование ФБО
FRU_PRS.1	Ограниченный приоритет обслуживания
FRU_RSA.1	Максимальные квоты
FTA_SSL.1	Блокирование сеанса, инициированное ФБО
FTA_SSL.2	Блокирование, инициированное пользователем
FTA_TAB.1	Предупреждение по умолчанию перед предоставлением доступа к ОО
FTA_TSE.1	Открытие сеанса с ОО
FTP_TRP.1	Доверенный маршрут

5.1.1.1 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	Генерация данных 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 журнала аудита	
FAU_STG.4	Предпринимаемые действия при сбое хранения журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на объекте, на который распространяется политика дискреционного управления доступом	Идентификатор объекта
FIA_AFL.1	Блокирование учетной записи в результате превышения максимального числа неуспешных попыток доступа к ОО	
FDP_IFC.1	Ограниченное управление информационными потоками	
FIA_SOS.1	Отклонение или принятие ФБО любого проверенного пароля	
FIA_UAU.2	Все случаи использования механизма аутентификации	
FIA_UID.2	Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	

Компонент	Событие	Детализация
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 ограничительных правил политики дискреционного управления доступом. 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	Модификация порового значения количества неуспешных попыток аутентификации	
FMT_REV.1 (1)	Все попытки отменить атрибуты безопасности, ассоциированные с пользователями ОО	
FMT_REV.1 (2)	Все попытки отменить атрибуты безопасности, ассоциированные с объектами	
FMT_SAE.1	Назначение срока действия для аутентификационных данных.	

Компонент	Событие	Детализация
	Блокирование ассоциированной с пользователем учетной записи	
FMT_SMR.1	Модификация группы пользователей – исполнителей роли пользователя ОО и администратора ОО. Каждое использование прав, предоставляемых ролью пользователя ОО и администратора ОО	Роль
FPT_AMT.1	Выполнение тестирования аппаратной среды и результаты тестирования	
FPT_STM.1	Изменения внутреннего представления времени	
FPT_TST.1	Выполнение и результаты самотестирования ФБО	
FTA_SSL.1	Все попытки разблокирования интерактивного сеанса	
FTA_SSL.2	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.2 «Идентификация до любых действий пользователя».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченному администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** 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 **уполномоченных администраторов ОО**, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны **предоставлять** возможность выполнить *поиск, сортировку* данных аудита, основанные на

[

следующих атрибутах:

а) идентификатор пользователя;

б) тип результата события (успех и/или отказ);

в) источник события;

г) категория события;

д) код события;

е) временной интервал совершения события;

ж) идентификатор учетной записи компьютера

].

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) тип результата события (успех и/или отказ);

в) источник события;

г) категория события;

д) код события;

е) временной интервал совершения события;

ж) идентификатор учетной записи компьютера

].

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 ОО], если журнал аудита превышает [определенный администратором ОО размер].

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 администратором ОО***, **или** [выполнить останов ОО] при переполнении журнала аудита.

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

5.1.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

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

[

а) субъектов – процессов, действующих от имени пользователей;

б) именованных объектов – рабочий стол (Desktop), событие (Event), пара событий (Event pair), порт завершения I/O (I/O Completion Port), задание (Job), ключ реестра (Key), почтовый ящик (Mailslot), именованный канал (Named pipe), каталог NTFS (NTFS directory), файл NTFS (NTFS file), каталог объектов (Object Directory), порт LPC (LPC Port), принтер (Printer), процесс (Process), секция (Section), семафор (Semaphore), символьная ссылка (Symbolic Link), поток (Thread), таймер (Timer), маркеры (Tokens), том (Volume), объект «Window Station» и объект службы каталогов (Active Directory objects);

в) операций между субъектами и объектами – обзор папок, выполнение файлов, содержание папки, чтение данных, чтение атрибутов, чтение дополнительных атрибутов, создание файлов, запись данных, создание папок, дозапись данных, запись атрибутов, запись дополнительных атрибутов, удаление, чтение разрешений, смена разрешений, смена владельца, удаление подпапок и файлов

].

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

[

а) ассоциированных с субъектом идентификаторе пользователя, принадлежности к группе (группам) и привилегиях субъекта;

б) следующих, ассоциированных с объектом атрибутах управления доступом:

[

– владелец объекта;

– список дискреционного управления доступом (DACL), который может отсутствовать, быть пустым, либо содержать одну или более записей; каждая запись в DACL содержит:

  – тип (разрешение или запрет);

  – идентификатор пользователя или группы;

  – право доступа к объекту;

установлены следующие правила доступа по умолчанию:

  – если DACL отсутствует, то к объекту разрешаются все виды доступа;

  – если DACL в наличии, но не содержит записей, то к объекту запрещены все виды доступа

]

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

доступ к объекту разрешен, если, по крайней мере, выполняется одно из следующих условий:

а) запись, содержащаяся в DACL, явно разрешает доступ пользователю, и доступ не был запрещен предыдущей записью, содержащейся в DACL;

б) запись, содержащаяся в DACL, явно разрешает доступ группе, членом которой является субъект, и доступ не был запрещен предыдущей записью, содержащейся в DACL;

в) список DACL отсутствует;

г) субъект является владельцем объекта и может просматривать или модифицировать список DACL или субъект является владельцем и может создавать объект

].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах:

[

а) при запросе уполномоченного администратора на доступ к объекту для смены владельца объекта, этот вид доступа должен быть ему предоставлен вне зависимости от правил, перечисленных в FDP_ACF.1.2;

б) при запросе уполномоченного администратора на смену или модификацию параметров аудита, фиксирующего попытки доступа к объектам ОО, этот вид доступа должен быть ему предоставлен вне зависимости от правил, перечисленных в FDP_ACF.1.2;

].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах:

[

в доступе к объекту должно быть явно отказано, если выполняется, по крайней мере, одно из следующих условий:

а) запись в списке DACL явно запрещает доступ для пользователя, и доступ не был разрешен предыдущей записью в DACL;

б) запись в списке DACL явно запрещает доступ группе, членом которой является пользователь, и доступ не был предоставлен предыдущей записью в DACL

].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_MSA.3 «Инициализация статических атрибутов».

FDP_IFC.1 Ограниченное управление информационными потоками

FDP_IFC.1.1 ФБО должны осуществлять [политику фильтрации информации] для

[

а) субъектов – субъектов, представляющих пользователей ОО; программ, функционирующих в среде ОО; внешних по отношению к ОО сущностей ИТ.

б) информации – входящего/исходящего в/из ОО информационного потока;

в) операций – перемещения информации

].

Зависимости: FDP_IFF.1 «Простые атрибуты безопасности».

FDP_IFF.1 Простые атрибуты безопасности

FDP_IFF.1.1 ФБО должны осуществлять [политику фильтрации информации], основанную на следующих типах атрибутов безопасности субъекта и информации:

[

а) атрибуты безопасности программы, функционирующей в среде ОО:

– имя программы;

б) атрибуты безопасности внешней по отношению к ОО сущности ИТ:

– предполагаемый адрес;

в) атрибуты безопасности информационного потока:

– предполагаемый адрес субъекта источника;

– протокол;

– номер порта

].

FDP_IFF.1.2 ФБО должны разрешать информационный поток между управляемым субъектом и **управляемой** информацией посредством управляемой операции, если выполняются следующие правила:

[

а) внешние по отношению к ОО сущности ИТ могут передавать информацию пользователям ОО, если:

– предполагаемый адрес внешней по отношению к ОО сущности ИТ является разрешенным;

– все значения атрибутов безопасности информационного потока являются разрешающими;

б) внешние по отношению к ОО сущности ИТ могут передавать информацию программам, функционирующим в среде ОО, если:

– предполагаемый адрес внешней по отношению к ОО сущности ИТ является разрешенным;
– имя программы, функционирующей в среде ОО, является разрешенным;
– все значения атрибутов безопасности информации являются разрешающими;

].

FDP_IFF.1.3 ФБО должны реализовать [дополнительные правила политики фильтрации информации не заданы].

FDP_IFF.1.4 ФБО должны предоставить следующее [дополнительные возможности политики фильтрации информации не заданы].

FDP_IFF.1.5 ФБО должны явно разрешать информационный поток, основываясь на следующих правилах: [основанные на атрибутах безопасности правила, которые явно разрешают информационные потоки, не заданы].

FDP_IFF.1.6 ФБО должны явно запрещать информационный поток, основываясь на следующих правилах: [основанные на атрибутах безопасности правила, которые явно запрещают информационные потоки, не заданы].

Зависимости: FDP_IFC.1 «Ограниченное управление информационными потоками», FMT_MSA.3 (2) «Инициализация статических атрибутов».

FDP_RIP.2 Полная защита остаточной информации

FDP_RIP.2.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания **ресурсов** при *<u>освобождении **ресурсов**</u>* для всех объектов.

Зависимости: отсутствуют.

5.1.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [установленное администратором ОО число] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного **в элементе FIA_AFL.1.1** числа неуспешных попыток аутентификации ФБО должны**:**

[

а) сделать невозможным доступ субъекта доступа к ОО, осуществив блокировку регистрационной записи на установленное время;

б) по истечении установленного времени осуществить сброс счетчика неуспешных попыток аутентификации

].

Зависимости: FIA_UAU.2 «Аутентификация до любых действий пользователя».

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) [привилегии и права входа].

].

Зависимости: отсутствуют.

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 ФБО должны предоставить механизм для верификации того, что **пароли на доступ к ОО** отвечают **следующей метрике качества**

[

а) минимальная длина – 8 символов;

б) пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

в) в пароле должны присутствовать символы как минимум трех категорий из числа следующих:

– прописные буквы английского алфавита от A до Z;

– строчные буквы английского алфавита от a до z;

– десятичные цифры от 0 до 9;
– символы, не принадлежащие алфавитно-цифровому набору;

].

Зависимости: отсутствуют.

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый **субъект доступа** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

FIA_UAU.7 Аутентификация с защищенной обратной связью

FIA_UAU.7.1 ФБО должны предоставлять **субъекту доступа** [возможность ввода аутентификационной информации в скрытом виде] во время выполнения аутентификации.

Зависимости: FIA_UAU.2 «Идентификация до любых действий пользователя».

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый **субъект доступа** был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

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) [привилегии].

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

а) [каждому субъекту будет назначено подмножество атрибутов безопасности, ассоциированных с пользователем, от имени которого субъект будет действовать].

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

а) [субъекты, действующие от имени пользователя, не могут присоединить дополнительные атрибуты безопасности помимо тех, которые были изначально назначены].

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

5.1.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны предоставлять возможность ***выполнять действия, указанные в третьем столбце таблицы 5.3,*** над функциями, [указанными во втором столбце таблице 5.3 в части управляемых характеристик, указанных в четвертом столбце таблицы 5.3], только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3 – Управляемые функции и характеристики безопасности

Компонент	Функции ФБО	Операция	Управляемая характеристика
FAU_SAR.1	аудит безопасности	удаление, модификация,	состав групп безопасности, имеющих привилегии на чтение

Компонент	Функции ФБО	Операция	Управляемая характеристика
		добавление	записей аудита
FAU_SEL.1	аудит безопасности	установление, просмотр, модификация	множество событий, подвергаемых аудиту
FAU_STG.3	аудит безопасности	установление, модификация	предпринимаемые действия при возможном сбое хранения журнала аудита
FAU_STG.4	аудит безопасности	удаление, модификация, добавление	предпринимаемые действия при переполнении журнала аудита
FIA_AFL.1	идентификация и аутентификация	установление, модификация	продолжительность блокировки регистрационной записи; временной интервал до осуществления сброса счетчика неуспешных попыток аутентификации
FIA_SOS.1	идентификация и аутентификация	установление, модификация	метрика качества паролей на доступ к ОО
FMT_MOF.1	управление безопасностью	удаление, модификация, добавление	состав групп безопасности, имеющих привилегии на управление функциями из числа ФБО
FMT_MSA.1	управление безопасностью	удаление, модификация, добавление	состав групп безопасности, имеющих привилегии на модификацию атрибутов безопасности
FMT_MSA.3	управление безопасностью	удаление, модификация, добавление	состав групп безопасности, имеющих привилегии на определение начальных значений
FMT_MTD.1	управление	удаление,	состав групп безопасности,

Компонент	Функции ФБО	Операция	Управляемая характеристика
	безопасностью	модификация, добавление	имеющих привилегии на модификацию данных ФБО
FMT_MTD.1	управление безопасностью	удаление, модификация, добавление	список пользователей, уполномоченных на модификацию собственных аутентификационных данных
FMT_MTD.2	управление безопасностью	удаление, модификация, добавление	состав групп безопасности, имеющих привилегии на модификацию порогового значения количества неуспешных попыток аутентификации
FMT_REV.1	управление безопасностью	удаление, модификация, добавление	состав групп безопасности, имеющих привилегии на отмену атрибутов безопасности, ассоциированных с пользователями ОО
FMT_SAE.1	управление безопасностью	удаление, модификация, добавление	состав групп безопасности, имеющих привилегии на назначение срока действия аутентификационных данных
FMT_SMR.1	управление безопасностью	удаление, модификация, добавление	состав пользователей ОО, являющихся участниками ролей уполномоченный администратор ОО и пользователь ОО
FPT_AMT.1	защита ФБО	установление, модификация	условия, при которых происходит тестирование аппаратного обеспечения ОО
FPT_TST.1	защита ФБО	установление, модификация	условия, при которых происходит самотестирование

Компонент	Функции ФБО	Операция	Управляемая характеристика
			ФБО
FRU_RSA.1	использование ресурсов	установление, модификация	квоты на томах файловой системы
FTA_SSL.1	блокирование сеанса	установление, модификация	интервал времени бездействия пользователя ОО и уполномоченного администратора ОО
FTA_TSE.1	доступ к ОО	установление, модификация	идентификатор пользователя; срок действия аутентификационных данных; время доступа

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность *модифицировать* [атрибуты управления доступом, ассоциированные с именованным объектом] только [пользователю ОО, являющемуся владельцем объекта; пользователю ОО, имеющему право смены владельца; пользователю ОО, имеющему право модификации DACL].

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 **позволять** [пользователю ОО, являющемуся владельцем объекта] определять альтернативные начальные значения для отмены значений по умолчанию при создании **объекта**.

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, очистка, [создание]* [журнала аудита] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (2) Управление данными ФБО

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

Зависимости: FMT_SMR.1 «Роли безопасности».

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».

FMT_MTD.1 (6) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *модификации* [продолжительности блокировки учетной записи пользователя после превышения порога неуспешных попыток аутентификации] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (7) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *модификации* [минимально допустимой длины пароля] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (8) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставить** возможность *модификации* [размер журнала аудита] только [уполномоченным администраторам].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.2 Управление ограничениями данных ФБО

FMT_MTD.2.1 ФБО должны предоставлять определение ограничений для [порогового значения количества неуспешных попыток аутентификации] только [уполномоченному администратору ОО].

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 ОО].

Зависимости: FMT_MTD.1 (1) «Управление данными ФБО»,
FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с ***пользователями*** в пределах ОДФ только [уполномоченному администратору ОО].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

а) немедленной отмены имеющих отношение к безопасности полномочий;

б) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с *объектами*, в пределах ОДФ только [пользователю ОО, уполномоченному согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

а) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SAE.1 Ограниченная по времени авторизация

FMT_SAE.1.1 ФБО должны **предоставлять** возможность назначать срок действия для [аутентификационных данных] только [уполномоченному администратору ОО].

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) пользователь

].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** 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».

5.1.1.5 Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ *при первоначальном запуске, периодически во время нормального функционирования, по запросу уполномоченного* ***администратора ОО*** для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая **является базовой для** ФБО.

Зависимости: отсутствуют.

FPT_ITC.1 Конфиденциальность экспортируемых данных ФБО при передаче

FPT_ITC.1.1 ФБО должны защищать все данные ФБО, передаваемые от ФБО удаленному доверенному продукту ИТ, от несанкционированного раскрытия при передаче.

Зависимости: отсутствуют.

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_RCV.1 Ручное восстановление

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

Зависимости: FPT_TST.1 «Тестирование ФБО»,
AGD_ADM.1 «Руководство администратора».

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 предоставлять надежные метки времени для собственного использования.

Зависимости: отсутствуют.

FPT_TST.1 Тестирование ФБО

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования *при запуске и периодически в процессе нормального функционирования* для демонстрации правильного выполнения ФБО.

FPT_TST.1.2 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО.

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

Зависимости: FPT_AMT.1 «Тестирование абстрактной машины».

5.1.1.6 Использование ресурсов (FRU)

FRU_PRS.1 Ограниченный приоритет обслуживания

FRU_PRS.1.1 ФБО должны установить приоритет каждому **субъекту ФБО**.

FRU_PRS.1.2 ФБО должны обеспечить доступ к [процессорному ресурсу] на основе приоритетов, назначенных **процессам**.

Зависимости: отсутствуют.

FRU_RSA.1 Максимальные квоты

FRU_RSA.2.1 ФБО должны реализовать максимальные квоты следующих ресурсов: [тома файловой системы], которые *отдельные пользователи* могут использовать *одновременно*.

Зависимости: отсутствуют.

5.1.1.7 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 пользователя ОО или уполномоченного администратора ОО], 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 ОО или уполномоченного администратора ОО].

Зависимости: FIA_UAU.1 «Выбор момента аутентификации».

FTA_SSL.2 Блокирование, инициированное пользователем

FTA_SSL.2.1 ФБО должны допускать инициированное пользователем **ОО или уполномоченным администратором ОО** 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 ОО или администратора ОО].

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 **следующем:**

[

а) идентификатор пользователя;

б) срок действия аутентификационных данных;

в) время доступа

].

Зависимости: отсутствуют.

FTA_TAB.1 Предупреждение по умолчанию перед представлением доступа к ОО

FTA_TAB.1.1 Перед открытием сеанса пользователя ФБО должны отобразить предупреждающее сообщение относительно несанкционированного использования ОО.

Зависимости: отсутствуют.

5.1.1.8 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 [и разблокирования сеанса].*

Зависимости: отсутствуют.

5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 ОК и образуют ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности ОО) (см. таблицу 5.4).

Таблица 5.4 – 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

5.1.2.1 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.

5.1.2.2 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.

5.1.2.3 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.

5.1.2.4 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 уполномоченному 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 уполномоченному 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.

5.1.2.5 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.

5.1.2.6 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. Краткая спецификация ОО

В данном подразделе представлено описание функций безопасности ОО и мер доверия к безопасности ОО, а также их сопоставление с требованиями безопасности для ОО.

6.1 Функции безопасности ОО

ОО реализует следующие функции безопасности:

- аудит безопасности;
- защита данных пользователя;
- идентификация и аутентификация;
- управление безопасностью;
- защита ФБО;
- использование ресурсов ОО;
- блокирование сеанса.

6.1.1 Функция безопасности «Аудит безопасности»

Функции безопасности ОО «Аудит безопасности» обеспечивают:

- сбор данных аудита;
- просмотр журнала аудита событий безопасности (журнала аудита);
- защиту журнала аудита событий безопасности от переполнения;
- ограничение доступа к журналу аудита событий безопасности.

6.1.1.1 Сбор данных аудита

В рамках ОО определено два компонента, выполняющие сбор данных аудита о событиях безопасности – справочный монитор безопасности SRM (Security Reference Monitor) и подсистема локальной аутентификации LSASS (Local Security Authority Subsystem Service).

На справочный монитор безопасности SRM (компонент исполнительной системы ОО) возложена функция генерации данных аудита для событий доступа к объекту, использования привилегий и отслеживания процессов. Генерация данных аудита для всех остальных категорий событий безопасности реализуется службами, выполняемыми в процессе LSASS. Единственным исключением из данных правил является случай

самостоятельной регистрации службой Event Logger (Регистратор событий) события очистки журнала аудита событий безопасности.

Определение категорий событий, подвергаемых аудиту, осуществляется через политику аудита, управление и модификация которой осуществляется только уполномоченными администраторами. Все параметры, определяемые в политике аудита, содержатся в базе данных политики безопасности, поддерживаемой подсистемой LSASS. В случае изменения администратором политики аудита подсистема LSASS актуализирует собственную базу данных политики безопасности и уведомляет об изменениях монитор безопасности SRM, который получает управляющий флаг, указывающий, что аудит разрешен, и структуру данных, определяющую категорию событий, подвергаемых аудиту.

За создание журнала аудита, содержащего записи аудита об относящихся к безопасности событиях, отвечает локальная служба «Регистратор событий» (Event Logger). Журнал регистрации событий безопасности содержит информацию о контролируемых политикой аудита событиях безопасности, таких как успешные и неуспешные попытки доступа к ОО, доступ к защищаемым активам, управление учетными данными пользователей и др.

В ОО реализован механизм подписки на получение записей событий аудита с удаленных компьютеров, что упрощает задачи определения, отслеживания и устранения неисправностей.

Использование журнала аудита позволяет отслеживать события безопасности, связанные с выполнением определенных действий или доступом к определенным объектам. Каждая запись в журнале аудита событий безопасности содержит сведения о выполненном действии, о пользователе, который его выполнил, а также о дате и времени события.

Объект оценки обеспечивает аудит как успешных, так и неуспешных попыток выполнения действий. При этом в журнал регистрации событий безопасности будут заноситься записи обо всех пользователях, которые пытались выполнить разрешенные или запрещенные для них действия. Каждое событие аудита представлено записью, содержащей следующие сведения (см. таблицу 6.1).

Таблица 6.1 – Сведения записей аудита

Сведения	Описание
Дата	Дата, соответствующая событию.

Сведения	Описание
Время	Время, когда произошло данное событие.
Пользователь	Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала аудита событий безопасности содержит оба кода.
Компьютер	Имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, если только просмотр событий не выполняется с другого компьютера.
Код события	Число, определяющее конкретный тип события. В первой строке описания обычно содержится название типа события. Код события и имя источника записи могут использоваться для устранения неполадок.
Источник	Программа, инициирующая событие. Это может быть как имя программы, так и название компонента системы или приложения, например, название драйвера. В случае журнала аудита событий безопасности источник события определяется как «Security».
Тип	Уровень важности событий. В журнале аудита событий безопасности записи событий могут быть двух типов – «Аудит успехов» и «Аудит отказов». Событие безопасности относится к типу «Аудит успехов», если соответствует успешно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае успешного входа пользователя в систему в журнал безопасности заносится событие аудита типа «Аудит успехов». Событие безопасности относится к типу «Аудит отказов», если соответствует отказу в доступе. Например, в случае неудачной попытке доступа пользователя к сетевому диску в журнал безопасности заносится событие аудита типа «Аудит отказов».
Категория	Категория события в зависимости от источника события. Для аудита событий безопасности категория соответствует одному из типов событий, для которых в политике аудита может быть включен аудит успехов или отказов.

Формат и содержание описания события аудита зависят от типа данного события. Описание события обычно содержит наиболее полезные сведения, относящиеся к причине и значимости события. В каждой записи аудита содержится информация, которая специфична для определенной категории контролируемого события. Описание данной информации представлено в таблице 6.2.

Таблица 6.2 – Информация записи аудита

№ п/п	Категория события	Описание
1.	Системное событие	Аудит событий, связанных с выполнением общесистемных операций, влияющих на безопасность ОО в целом или на журнал безопасности (например, переполнение или очистка журналов аудита)
2.	Доступ к объектам	Аудит попыток доступа к объектам, таким как файлы, папки или принтеры. Отслеживание данного типа событий предполагает явное определение администратором тех видов операций, которые при выполнении пользователями будут зафиксированы в журнале аудита.
3.	Использование привилегий	Аудит событий, связанных с использованием дополнительных привилегий, относящихся к безопасности. К таковым относят привилегии, связанные с ФБО и, которые могут быть назначены соответствующим субъектам в эквивалентной конфигурации.
4.	Отслеживание процессов	Аудит событий, связанных с запуском, выполнением или прекращением работы каких-либо сервисов или приложений.
5.	Изменение политики	Аудит событий, связанных с изменением

№ п/п	Категория события	Описание
		параметров и настроек политик безопасности, прав доступа на выполнение общесистемных операций и изменением режимов работы самой системы аудита.
6.	Управление учетной записью	Аудит событий, связанных с созданием, удалением или изменением учетных записей пользователей или групп, а также изменением их атрибутов.
7.	Доступ к службе каталогов	Аудит событий доступа к объектам службы каталогов и соответствующим атрибутам данных объектов.
8.	События входа в систему	Аудит событий, связанных с регистрацией пользователей в ОО, в случае, когда контроллер домена получил запрос на проверку правильности учетной записи пользователя.
9.	Вход в систему	Аудит событий, связанных с входом/выходом пользователя в/из системы, попытками установить сетевое подключение.

В рамках каждой категории событий аудита могут определяться типы контролируемых событий, указывающие, какие попытки отслеживать: успешные или неуспешные, либо совместно те и другие. Для реализации аудита событий доступа к объектам дополнительно необходимо определить, какие типы доступа и какие пользователи или группы подлежат контролю. Задание типов доступа и идентификаторов пользователей или групп пользователей осуществляется посредством системных списков управления доступом SACL (System Access Control List) – списков назначений аудита. Списки назначений аудита SACL привязаны к объекту и указывают на необходимость аудита событий доступа к конкретным объектам или атрибутам объектов (в случае доступа к объектам службы каталогов Active Directory).

6.1.1.2 Просмотр журналов аудита

Инструментальное средство ОО «Просмотр событий» (Event Viewer) предоставляет пользовательский интерфейс для просмотра содержимого журнала безопасности на локальном и удаленном компьютере, а также возможность поиска и фильтрации конкретных событий аудита. Для журнала безопасности в качестве параметров фильтрации и поиска событий могут быть заданы: идентификатор пользователя, тип события, источник события, категория события, код события, временной интервал, за который необходимо просмотреть события, и имя компьютера.

6.1.1.3 Защита журнала аудита от переполнения

Объект оценки предотвращает потерю данных аудита событий безопасности посредством управления регистрацией и очередью событий аудита. Исходя из настроек ОО, данные аудита добавляются в журнал аудита событий безопасности до тех пор, пока он не станет полным. ОО обеспечивает защиту данных аудита от потери, используя возможность генерировать событие аудита в случае, если размер журнала аудита безопасности достигнет установленного для него порогового значения. Кроме того, уполномоченный администратор может сконфигурировать ОО на запрет затирания данных аудита (т.е. очистка журнала аудита событий безопасности будет осуществляться вручную) или немедленное завершение работы в случае переполнения журнала аудита событий безопасности. При такой конфигурации, в случае завершения работы ОО в результате переполнения журнала аудита событий безопасности, повторную регистрацию в ОО может выполнить только уполномоченный администратор. В случае заполнения журнала на дисплей администратора выводиться сообщение, указывающие, что произошло переполнение журнала аудита.

Управление максимальным размером журнала безопасности, временем, в течение которого должны сохраняться имеющие важность события, и способом сохранения событий в журнале безопасности может осуществляться посредством редактирования свойств журнала безопасности либо через использование групповой политики, позволяющей централизовано определять единые параметры для журналов регистрации событий безопасности.

ФБО обеспечивают сбор информации о событиях безопасности посредством справочного монитора безопасности SRM и подсистемы LSASS. Оба компонента подсистемы безопасности ОО поддерживают собственные очереди событий аудита.

Монитор безопасности SRM помещает записи аудита во внутреннюю очередь для последующей их передаче подсистеме LSASS, которая со своей стороны поддерживает вторую очередь, содержащую в себе данные аудита, переданные монитором безопасности SRM и другими службами. Обе очереди событий аудита отслеживают возможную потерю данных аудита. Монитор безопасности SRM определяет верхнюю и нижнюю метку для собственной очереди событий аудита, что позволяет отследить момент ее заполнения. Подсистема LSASS также поддерживает метки для собственной очереди событий аудита с целью определения момента ее заполнения.

Потеря данных аудита может произойти в случае, если очереди подсистемы LSASS и монитора безопасности SRM достигнут установленных для них значений верхних меток, либо в случае, когда размер файла журнала аудита событий безопасности достигнет своего предела.

6.1.1.4 Ограничение доступа к журналу аудита

Служба «Регистратор событий» обеспечивает управление и защиту журнала аудита безопасности. Чтобы просмотреть содержимое журнала, пользователь должен быть в роли уполномоченного администратора. Журнал регистрации событий безопасности является системным ресурсом, создаваемым на этапе установки системы. ОО не располагает интерфейсами, позволяющими создавать, удалять или изменять журнал регистрации событий безопасности. Подсистема локальной аутентификации LSASS является единственной службой, обеспечивающей запись событий в журнал аудита событий безопасности.

Сопоставление с ФТБ

Функции безопасности «Аудит безопасности» удовлетворяют следующим функциональным требованиям безопасности:

- FAU_GEN.1 – ОО обеспечивает генерацию данных аудита для всех категорий событий, представленных в таблице 6.2. Для каждого события аудита ФБО регистрируют дату, время, идентификатор пользователя или его имя, идентификатор события, источник, тип и категорию события;
- FAU_GEN.2 – ФБО обеспечивают ассоциирование каждого события, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события;

- FAU_SAR.1 – инструментальные средства просмотра событий предоставляют уполномоченному администратору ОО возможность просмотра данных аудита в удобочитаемом формате;
- FAU_SAR.2 – ФБО предоставляют доступ к чтению записей аудита только уполномоченным администраторам ОО;
- FAU_SAR.3 – инструментальные средства просмотра событий аудита предоставляют возможность выполнения поиска и сортировки данных аудита по идентификатору пользователя, типу результата события (успех и/или отказ), источнику события, категории события, коду события, временному интервалу совершения события, идентификатору учетной записи компьютера;
- FAU_SEL.1 – ФБО предоставляют возможность включать события, потенциально подвергаемые аудиту, в совокупность событий, подвергающихся аудиту;
- FAU_STG.1 – ФБО защищают хранимые записи аудита от несанкционированного изменения и предотвращают их модификацию;
- FAU_STG.3 – ОО может быть настроен на генерацию события аудита (предупреждение о превышении размера) в случае превышения данными аудита установленного для журнала безопасности размера;
- FAU_STG.4 – ОО может быть настроен на предотвращение генерации событий аудита или выполнение аварийного останова в случае переполнения журнала аудита;
- FMT_MTD.1(8) – ФБО предоставляют возможность устанавливать размер журнала аудита безопасности только уполномоченным администраторам.

6.1.2 Функции безопасности «Защита данных пользователя»

К предоставляемым ОО механизмам обеспечения защиты данных пользователя относятся:

- дискреционное (избирательное) управление доступом;
- контроль учетных записей пользователей (UAC);
- фильтрация информации;
- защита остаточной информации.

6.1.2.1 Дискреционное управление доступом

ФБО обеспечивают опосредованный доступ между субъектами и объектами данных пользователя (именованными объектами). Субъекты доступа представлены набором процессов с одним или несколько потоками, выполняющимися от имени пользователей и в контексте их безопасности, т.е. в рамках определенных для пользователей полномочий. В таблице 6.3 представлен перечень объектов данных пользователя, на которые распространяется политика дискреционного управления доступом, устанавливаемая для ОО.

Таблица 6.3 – Перечень объектов, на которые распространяется политика дискреционного управления доступом

№ п/п	Именованные объекты	Описание
1.	Рабочий стол (Desktop)	Основной объект, содержащийся в объекте типа WindowStation.
2.	Событие (Event)	Объект, создаваемый для механизма межпроцессного взаимодействия IPC (Interprocess Communication). Может пребывать либо в свободном, либо в занятом состоянии. Используется для синхронизации или уведомления.
3.	Пара событий (Event Pair)	Объект, создаваемый для механизма межпроцессного взаимодействия.
4.	Порт завершения ввода/вывода (I/O Completion Port)	Метод постановки в очередь и извлечения из нее уведомлений о завершении операций ввода/вывода.
5.	Задание (Job)	Совокупность процессов, управляемых как единая группа.
6.	Раздел реестра (Registry Key)	Механизм ссылки на данные в реестре. С объектом «раздел реестра» может быть сопоставлено произвольное количество параметров.
7.	Мьютекс (Mutex)	Механизм синхронизации, используемый для упорядочения доступа к ресурсам.

№ п/п	Именованные объекты	Описание
8.	Порт LPC (LPC port)	Объект механизма вызова локальных процедур.
9.	Почтовый ящик (Mail slot)	Объект ввода/вывода, предоставляющий механизм ненадежного одностороннего широковещания.
10.	Именованный канал (Named Pipe)	Объект ввода/вывода, используемый для обеспечения надежной двусторонней связи через сеть.
11.	Каталог NTFS (NTFS Directory)	Объект файловой системы NTFS.
12.	Файл NTFS (NTFS file)	Файл данных пользователя, управляемый NTFS.
13.	Принтер (Printer)	Представление конкретной очереди печати и всех соответствующих ей устройств печати.
14.	Каталог AD (Active Directory)	Представление общих ресурсов, определяемых и поддерживаемых службой каталогов Active Directory.
15.	Процесс (Process)	Совокупность потоков, выполняющихся в едином контексте и имеющих общее виртуальное адресное пространство и управляющую информацию.
16.	Секция (Section)	Область памяти.
17.	Семафор (Semaphore)	Счетчик, действующий как шлюз к ресурсам. Позволяет указывать максимальное число потоков, которым разрешен доступ к защищенным этим объектом ресурсам.
18.	Символьная ссылка (Symbolic Link)	Механизм косвенной ссылки на имя объекта.
19.	Поток (Thread)	Представляет исполнительную часть процесса. Все потоки в пользовательском режиме ассоциированы с процессами.
20.	Таймер (Timer)	Механизм уведомления потока об истечении фиксированного периода времени.
21.	Маркер доступа (Access Token)	Представляет контекст безопасности процессов или потоков.

№ п/п	Именованные объекты	Описание
22.	Том (Volume)	Один или несколько разделов, отформатированных для использования файловой системой.
23.	Объект «Window-Station»	Объект, содержащий буфер обмена и группу объектов «рабочий стол».

Атрибуты субъектов дискреционного управления доступом

К атрибутам субъектов дискреционного управления доступом относят маркеры доступа (access token), содержащие набор атрибутов безопасности для каждого субъекта. Маркеры доступа ассоциируются с каждым процессом или потоком, выполняемым от имени определенного пользователя, и определяет их контекст безопасности.

В процессе регистрации в ОО служба Winlogon создает начальный маркер доступа, представляющий пользователя, который входит в ОО, и сопоставляет его с процессом оболочки – пользовательским интерфейсом. Далее все программы, запускаемые пользователем, наследуют копию этого маркера.

Длина маркеров может варьироваться для различных субъектов доступа, поскольку учетные записи разных пользователей имеют неодинаковые наборы привилегий и являются участниками различных групп безопасности. Маркер доступа включает следующие основные элементы:

- идентификатор безопасности SID пользователя;
- идентификаторы безопасности соответствующих групп безопасности, членами которых является данный пользователь;
- назначенные пользователю привилегии;
- устанавливаемый по умолчанию дискреционный список управления доступом для создаваемых пользователем объектов;
- идентификатор безопасности владельца;
- тип маркера (основной или имперсонированный);
- уровень имперсонации (для имперсонированных маркеров);
- идентификатор сеанса;
- источник маркера;
- идентификатор маркера;

– атрибут политики аудита;
– атрибут происхождения маркера доступа (Origin).

ФБО для определения набора разрешенных субъекту действий используют два элемента маркера доступа. Первый включает в себя идентификатор безопасности SID учетной записи пользователя и групп безопасности, участниками которых он является. Используя идентификаторы безопасности, справочный монитор безопасности SRM определяет возможность предоставления субъекту запрашиваемого типа доступа к защищаемому объекту (например, объектам файловой системы NTFS). Вторым элементом маркера доступа определяющим, что может делать субъект, которому назначен данный маркер, является список привилегий – набор назначенных пользователю прав на выполнение определенных действий в системе.

Устанавливаемый по умолчанию дискреционный список управления доступом DACL представляет собой атрибуты безопасности, применяемые ОО в отношении создаваемых субъектом доступа (процессом или потоком) объектов. Включая в маркеры доступа указанную информацию, ОО упрощает процессам и потокам создание объектов со стандартными атрибутами безопасности, так как в этом случае им не требуется запрашивать информацию о списках DACL при создании каждого объекта доступа.

Маркеры доступа, поддерживаемые ОО, разделяются на основные (primary access token), т.е. определяющие контекст безопасности субъектов доступа (процесса или потока), и имперсонированные (impersonation access token), применяемые в случае, когда контекст безопасности потока должен отличаться от контекста безопасности его процесса.. При имперсонации механизмы контроля доступа и генерации данных аудита используют вместо маркера родительского процесса контекст безопасности потока, а без имперсонации – контекст безопасности родительского процесса, которому принадлежит поток. В результате данный поток имперсонирует (олицетворяет) субъекта, предоставившего имперсонированный маркер доступа. Механизм имперсонации прекращает действовать, когда имперсонированный маркер удаляется из потока или при завершении потока.

В случае существования у потока имперсонированного маркера доступа управление доступом осуществляется на его основе, в противном случае – на основе первичного маркера доступа процесса, в рамках которого выполняется поток.

Ограниченные маркеры

В ОО помимо основных и имперсонированных маркеров доступа различают ограниченные маркеры (restricted token). Ограниченный маркер доступа создается на базе основного или имперсонированного маркера и является его точной копией, в которую можно внести следующие изменения:

- удалить некоторые элементы из таблицы привилегий, предоставленных субъекту доступа;
- пометить идентификаторы безопасности SID, содержащиеся в маркере, атрибутом проверки только на запрет (deny-only);
- пометить идентификаторы безопасности SID-идентификаторы, содержащиеся в маркере, как ограниченные (restricted SID).

Ограниченные маркеры используются в случаях, когда приложение подменяет контекст безопасности субъекта при выполнении небезопасного кода. Например, в ограниченном маркере может отсутствовать привилегия на перезагрузку системы, что не позволит коду, выполняемому в контексте безопасности, формируемом ограниченным маркером доступа, перезагрузить систему.

Атрибуты объектов дискреционного управления доступом

К атрибутам объектов дискреционного управления доступом относят дескрипторы безопасности (security descriptor), которые содержат все атрибуты безопасности, ассоциированные с объектом. К атрибутам безопасности, содержащимся в дескрипторе безопасности, относятся:

- номер версии;
- идентификатор безопасности SID владельца объекта;
- управляющие флаги, определяющие поведение или характеристики дескриптора безопасности;
- дискреционный список управления доступом, содержащий информацию о разрешениях и запретах, установленных для данного объекта (DACL);
- системный список управления доступом, содержащий строки назначений аудита (SACL).

Элементами дискреционного списка управления доступом являются записи управления доступом ACE (Access Control Entry). Каждая запись ACE определяет:

- идентификатор безопасности пользователя и группы безопасности, для которых определены разрешения доступа;
- маску доступа – разрешения, предоставленные определенному пользователю или группе безопасности;
- значения разрешений (разрешить/запретить).

Существуют два типа строк управления доступом ACE:

1. ALLOW ACEs – разрешающие строки, разделяющиеся на:
   - ACCESS_ALLOWED_ACE («доступ разрешен» (access allowed)) – используется для назначения прав доступа пользователям или группам пользователей;
   - ACCESS_ALLOWED_OBJECT_ACE («разрешенный объект» (allowed-object)) – используется для назначения прав доступа пользователям или группе пользователей к отдельным атрибутам объектов службы каталогов Active Directory, либо для ограничения наследования записей ACE для определенных типов дочерних объектов. Данный тип записей ACE поддерживается только для объектов службы каталога Active Directory.
2. DENY ACEs – запрещающие строки, разделяющиеся на:
   - ACCESS_DENIED_ACE («доступ отклонен» (access denied)) – используется для запрета доступа пользователям или группе пользователей;
   - ACCESS_DENIED_OBJECT_ACE («запрещенный объект» (denied-object)) – используется для запрета доступа пользователям или группе пользователей к отдельным атрибутам объектов службы каталогов Active Directory, либо для ограничения наследования записей ACE для определенных типов дочерних объектов. Данный тип записей ACE поддерживается только для объектов службы каталога Active Directory.

Механизм проверки прав доступа

Модель защиты объекта оценки требует, чтобы субъект доступа заранее - еще до доступа к объекту – указывал, какие операции он собирается выполнять над данным объектом. Система проверяет тип доступа, запрошенный субъектом (потоком), и, если такой доступ ему разрешен, он получает описатель, позволяющий ему выполнять операции над объектом. Когда субъект (поток) создает объект или открывает описатель

существующего объекта, он должен указать маску запрашиваемых прав доступа (desired access rights), определяющих действия, которые субъект доступа намеревается выполнить в отношении указанного объекта.

Маска доступа определяет права доступа с привязкой к конкретному идентификатору безопасности пользователя или группы пользователей и используется для определения запрашиваемого и назначенного доступа к объекту. Каждый бит в маске доступа представляет конкретное право доступа.

Существует четыре категории прав доступа: стандартные, специальные, особые и общие. Стандартные права доступа применимы ко всем типам объектов. Специальные права доступа в зависимости от типа объекта принимают различное семантическое значение. Так в случае объекта «файл» субъект может запросить права на удаление файла или добавления данных в файл, а в случае объекта «поток» – права на остановку потока или его завершение. Особые права доступа используются в масках запрашиваемого доступа для запроса особого доступа или всех допустимых прав. Общие права доступа применяются для группировки стандартных и особых прав доступа. Каждый тип объектов обеспечивает самостоятельное сопоставление общих прав доступа со стандартными и особыми правами.

Для большинства объектов, субъект, запросив доступ к объекту (например, открытие файла), получает в ответ указатель на описатель (handle). Когда субъект доступа открывает описатель объекта, диспетчер объектов вызывает так называемый справочный монитор безопасности SRM и посылает ему уведомление о наборе запрашиваемых субъектом прав доступа. Далее, монитор безопасности SRM проверяет, разрешает ли дескриптор безопасности объекта, выполнять с объектом действия, указанные в маске запрашиваемого доступа. В случае положительного результата проверки, субъекту доступа справочным монитором безопасности SRM возвращается маска предоставленных прав доступа (granted access rights), информацию о которых диспетчер объектов сохраняет в созданном им описателе объекта, т.е. осуществляется ассоциация маски назначенного доступа с каждым открытым описателем

После этого при осуществлении повторных попыток доступа, диспетчер объектов может быстро проверить соответствие набора предоставленных прав доступа, хранящихся в описателе объекта, действиям, которые намеревается выполнить субъект.

Для объектов в режиме ядра описатели представлены в таблице описателей (handle table) режима ядра. Для каждого процесса определена своя таблица описателей, каждая

строка которой идентифицирует открытый объект и права доступа, назначенные для данного объекта. В пользовательском режиме механизм использования описателей аналогичен режиму ядра, т.е. с помощью таблицы описателей определяется расположение необходимого объекта и ассоциированная с ним маска назначенного доступа. В обоих случаях, и для объектов пользовательского режима, и для объектов режима ядра, контроль доступа реализуется монитором безопасности SRM.

Для некоторых объектов, в частности объектов службы каталогов, ОО не поддерживают механизм описателей. В этих случаях, проверка доступа выполняется по каждой ссылке к объекту. Объекты службы каталогов также отличаются от других объектов тем, что имеют дополнительные атрибуты. Аналогично остальным объектам, объекты службы каталогов имеют дескриптор безопасности, однако таблица DACL данных объектов может содержать записи ACE, определяющие права доступа к определенным атрибутам данных объектов, а не ко всему объекту в целом.

Алгоритм реализации политики дискреционного управления доступом

Объект оценки реализует политику дискреционного управления доступом к объектам, основываясь на идентификаторах безопасности и привилегиях, представленных в маркере доступа запрашивающего субъекта доступа, маске запрашиваемого доступа и дескрипторе безопасности объекта.

Представленный ниже алгоритм дает краткое описание механизма принятия решения о разрешении доступа к объекту данных пользователя. Для того чтобы предоставить субъекту доступ к объекту, необходимо выполнить проверку прав его доступа, указанных в маске запрашиваемого доступа. Проверка прав выполняется по шагам в порядке следования записей управления доступом ACE до первого запрета на какую-либо операцию или до явного разрешения всех запрошенных операций. В случае если все строки просмотрены, но осталось хотя бы одно право, не разрешенное явно, доступ будет запрещен.

1. **Наличие дискреционного списка управления доступом**

В случае отсутствия списка DACL (DACL = Null) объект доступа является незащищенным. В дальнейшем все требуемые права доступа субъекту будут предоставлены.

2. **Проверка привилегий**

Проверка привилегии SeTakeOwnershipPrivilege – если маркер доступа запрашивающего субъекта содержит привилегию SeTakeOwnershipPrivilege, дающую

право на изменение дескриптора безопасности объекта в части смены его владельца, ОО предоставляет субъекту право на доступ «запись владельца» (WRITE_OWNER) до анализа списка DACL.

3. Проверка владельца объекта (Owner)

Проверка всех идентификаторов безопасности, указанных в маркере доступа, с целью определения совпадения с идентификатором безопасности владельца объекта. Если соответствие между идентификаторами безопасности установлено, то при необходимости субъекту могут быть предоставлены право управления изменением дискреционного списка управления доступом (WRITE_DACL) и право управления чтением информации из дескриптора безопасности объекта, за исключением списка назначений аудита (READ_CONTROL).

Тот факт, что владелец объекта всегда получает право на запись списка DACL при доступе к объекту, означает, что субъектам нельзя запретить доступ к принадлежащим им объектам. Если в силу каких-то причин список DACL объекта пуст, что означает запрет на доступ к указанному объекту каких-либо субъектов доступа, владелец может осуществить доступ к объекту с правом записи DACL и определить необходимые права доступа.

4. Проверка содержимого дискреционного списка управления доступом

В случае если дискреционный список управления доступом представлен, но не содержит записей ACE, в доступе субъекта к объекту будет отказано.

5. Итеративный процесс проверки каждой записи ACE, согласно порядку их представления в дискреционном списке управления доступом

Если атрибуты наследования записи ACE указывают, что областью применения данной записи являются только дочерние объекты, она пропускается.

Если идентификатор безопасности в записи ACE не совпадает ни с одним идентификатором, представленным в маркере доступа запрашивающего субъекта, запись ACE пропускается.

Если идентификаторы безопасности SID совпали, осуществляется формирование маски предоставленных прав доступа:

- из маски предоставленных прав доступа удаляется маска доступа каждой записи ACE типа «доступ отклонен» (ACCESS_DENIED_ACE);
- к маске предоставленных прав доступа добавляется маска доступа каждой записи ACE типа «доступ разрешен» (ACCESS_ALLOWED_ACE). Исключение составляют права доступа, в предоставлении которых было уже отказано.

6.1.2.2 Контроль учетных записей пользователей (UAC)

Контроль учетных записей пользователей (User Account Control, UAC) – это средство предотвращения несанкционированного запуска вредоносных программ и изменения системных и пользовательских данных.

Контроль обеспечивает пересмотр списка стандартных возможностей пользователя, путем включения в него множества базовых функций, которые не несут риска нарушения безопасности ОО, хотя в предыдущих версиях ОС Windows, требовали административных привилегий (например, изменение временной зоны, изменение настройки экрана, добавление принтера). Если пользователь или приложение пытается выполнить действие, для которого требуются полномочия администратора (например, установка нового приложения или изменение системных параметров), то появляется окно UAC с требованием ввести пароль администратора. Кроме этого, UAC позволяет пользователям с административными правами работать в более безопасной среде путем ограничения (по умолчанию, администраторы имеют минимальные права)доступа к критическим ресурсам и функциям ОС. Если для выполнения какой-либо задачи требуются повышенные привилегий, то ОО с помощью окна UAC запросит подтверждения выполнение данной задачи. В целях повышения безопасности при появлении окна UAC экран компьютера блокируется.

Для обеспечения защиты и нормальной работы приложений, требующих для своего выполнения административных привилегий, ОО содержит механизм виртуализации файловой системы и системного реестра, т.е. изменения, вносимые в виртуализованные настройки реестра и папок, доступны только под той учетной записью пользователя, который внес эти изменения, и в приложениях, запущенных под его учетной записью.

6.1.2.3 Фильтрация информации

ФБО обеспечивают защиту компьютера, непосредственно подключенного к сети, от сетевых атак различных типов.

ФБО обеспечивают проверку допустимости каждой попытки передачи/получения данных в процессе организации информационного обмена с внутренней или внешней вычислительными сетями. Поддерживая таблицу состояния активных соединений (stateful inspection), ФБО позволяют отслеживать все характеристики передаваемого трафика и

проверять исходный адрес и адрес назначения в каждом обрабатываемом сообщении, и используют полученную информацию, чтобы определить, какие сетевые пакеты разрешаются получать ОО. ФБО автоматически разрешают все исходящие соединения, независимо от программ и контекста безопасности, в котором они функционируют.

Чтобы исключить несанкционированную передачу информационных потоков из внешних вычислительных сетей и получение незапрашиваемых входящих запросов, поступающих из внутренней вычислительной сети, ОО ведет таблицу всех исходящих сеансов связи, инициированных с компьютера, на котором он установлен. Весь входящий трафик из внешней/внутренней вычислительных сетей проверяется по записям таблицы, поддерживаемой ОО. Этот трафик пропускается на компьютер только в том случае, если в таблице имеется соответствующая запись, показывающая, что обмен данными был начат с данного компьютера. В противном случае сеансы связи, инициируемые из источников, находящихся с внешней стороны компьютера, блокируются.

Помимо этого, в процессе регулирования обмена данными учитываются дополнительные параметры (списки исключений и ограничения), определяющие поведение ФБО и задаваемые администратором ОО исходя из среды функционирования ОО и выполняемых им задач. Передача/получение сетевых пакетов ОО в/из вычислительной сети разрешается только при условии успешного завершения всех проверок.

В случае попытки подключения из вычислительных сетей к ОО с задействованными механизмами обеспечения сетевой безопасности последний выполняет одно из следующих действий:

- блокирует подключение;
- разрешает подключение.

Поведение ФБО определяется списком исключений, задаваемых для программ и портов, которые определяются самостоятельно администратором ОО для каждого ОО, а также рядом других установленных параметров.

При задании списка исключения для программ администратор ОО определяет перечень программ, которым разрешается получение незапрашиваемых входящих запросов по любому порту, которые они пытаются открыть. Автоматическое открытие и закрытие требуемых портов осуществляется независимо от контекста безопасности функционирующего в ОО приложения. При этом приложение, включенное в список

исключений для программ, может открывать только необходимые для его правильного функционирования порты и только на то время, на которое оно их задействует.

В случае, когда определен список исключений для портов, ФБО разрешают непредусмотренные запросы на подключение к персональному компьютеру для конкретной программы или службы через разрешенный порт.

Использование параметров IP-безопасности позволяет настроить способы обеспечения безопасности при обмене ключами, параметры защиту данных (целостность и шифрование) в правилах подключения при защите сетевого трафика и проверку подлинности в соответствии с требованиями среды.

6.1.2.4 Защита остаточной информации

Объект оценки обеспечивает недоступность предшествующего информационного содержания ресурсов при распределении их субъектам и объектам, гарантируя, что ресурсы, выделяемые процессам в пользовательском режиме, не имеют остаточной информации, и процессы не смогут прочитать или восстановить их содержимое. В первую очередь это затрагивает процесс управления памятью, выделяемой процессам.

Механизм управления памятью реализует как изоляцию адресных пространств процессов, так и очистку памяти при ее освобождении. Обеспечение изоляции адресных пространств процессов реализуется выделением для каждого процесса отдельной директории страниц физической памяти и невозможностью прямого изменения процессом этой директории и других структур управления памятью.

Основными элементами управления памятью являются (см. рисунок 6.1):

- контексты страниц процессов;
- диспетчер памяти;
- страничная база диспетчера.

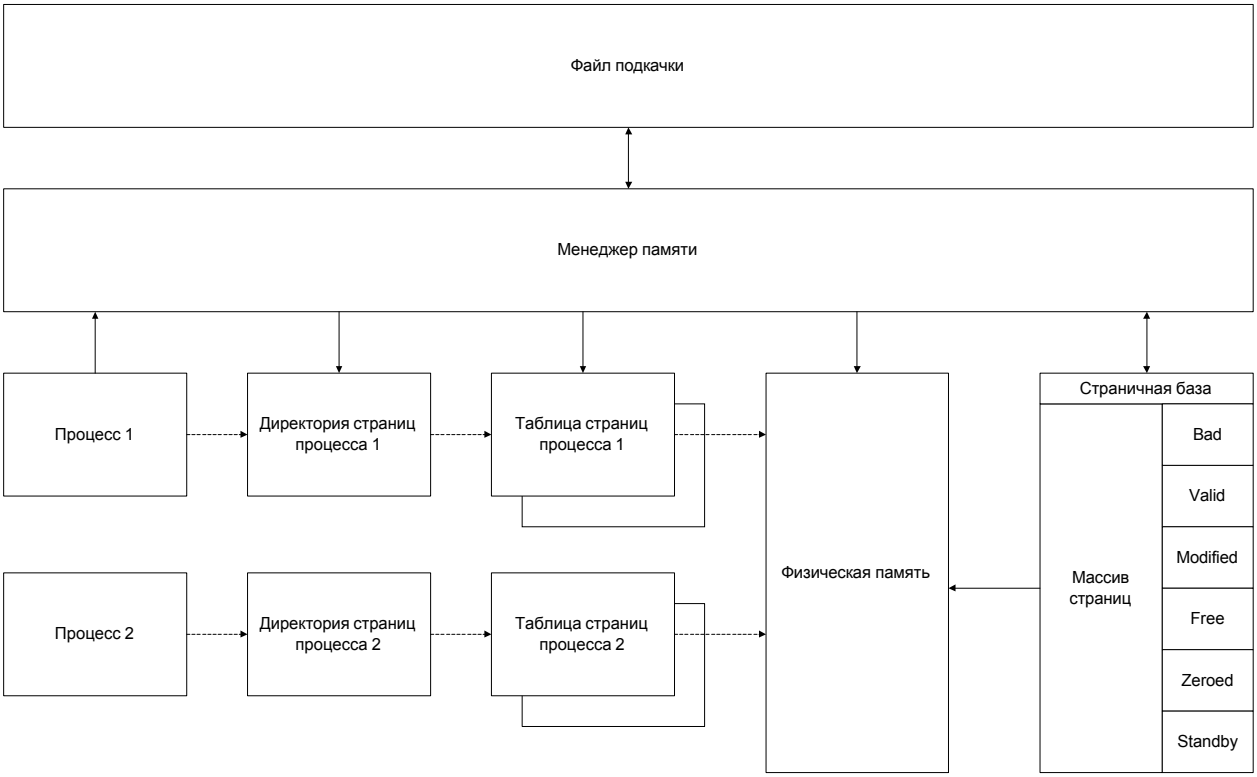

Рисунок 6.1 – Структура управления памятью ОО

Контекст страниц процесса представляет собой структуры данных, на которые ссылается контекст процесса, и используется для аппаратной трансляции абстрактных адресов. Контекст состоит из:

- директории страниц процесса, которая содержит ссылки (PDE) на таблицы страниц процесса на основе первых 10 бит виртуального адреса;
- таблиц страниц процесса, которые содержат ссылки (PTE) на страницы физической памяти на основе вторых 10 бит виртуального адреса;
- кэша трансляции (TLB), который содержит ссылки на наиболее часто используемые страницы физической памяти.

Контекст страниц процесса заполняется и модифицируется диспетчером памяти при создании процесса, переключении задач, выполнении запросов на выделение и освобождение памяти, а также при изменении состояния страничной базы. Контекст страниц является системной структурой и недоступен из контекста самого процесса.

Диспетчер памяти ОО является отдельным системным процессом, отвечающим за:

- поддержание, модификацию и переключение контекстов страниц процессов;

– обработку запросов на актуализацию страниц физической памяти и страничного файла;
– обработку запросов процессов на выделение и освобождение памяти;
– в своей работе диспетчер памяти использует страничную базу для хранения информации о состоянии страниц физической памяти.

Страничная база диспетчера памяти представляет собой системную структуру данных, используемую диспетчером памяти и содержащую информацию о состоянии страниц физической памяти. Страничная база состоит из массива доступных страниц памяти и связанных списков индексов массива по состоянию страниц. Списки индексов служат для ускорения поиска страниц с определенным состоянием и включают:

1. *Используемые (Valid) страницы* – страницы, с которыми работаю процессы.
2. *Исправленные (Modified) страницы* – страницы, в которые осуществлялась запись в физической памяти и подлежащие актуализации в страничном файле.
3. *Ожидающие (Standby) страницы* – страницы, которые ожидают удаления из контекста процесса.
4. *Свободные (Free) страницы* – страницы, освобожденные процессом и ожидающие обнуления.
5. *Обнуленные (Zeroed) страницы* – страницы, освобожденные и обнуленные, доступные к выделению процессам.
6. *Испорченные (Bad) страницы* – страницы памяти, содержащие сбойные адреса физической памяти.

Единственным процессом, модифицирующим страничную базу, является диспетчер памяти ОО. Модификация страничной базы включает изменение флагов состояния страниц и списков индексов в ответ на соответствующие события в системе. Граф переходов состояния страниц приведен на рисунке 6.2. При изменении состояния страницы происходит не только изменение ее флагов, но и модификация соответствующих списков индексов.

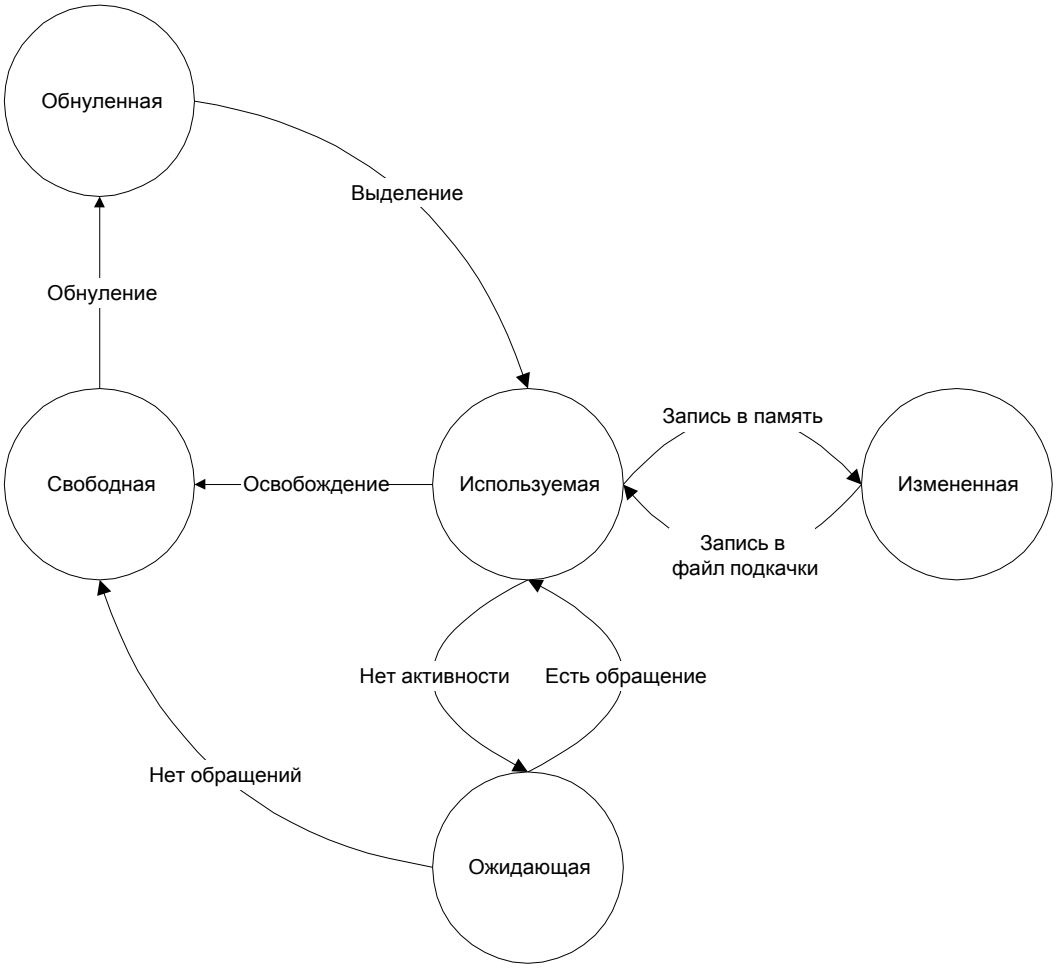

Рисунок 6.2 – Граф переходов состояний страниц памяти, управляемой ОО

Переходы между состояниями страницы осуществляются при следующих условиях:

1. *Обнуленная* → *используемая* – при запросе на выделение памяти или актуализации выгруженной информации.
2. *Используемая* → *измененная* – при изменении содержания страницы.
3. *Измененная* → *используемая* – после актуализации информации в файле подкачки.
4. *Используемая* → *ожидающая* – периодически переходит для уменьшения рабочего набора процесса.
5. *Ожидающая* → *используемая* – при обращении процесса к странице.
6. *Ожидающая* → *свободная* – при отсутствии обращений к странице.
7. *Свободная* → *обнуленная* – после обнуления.

Изменение состояния страницы производится диспетчером памяти посредством основных двух способов: при генерации прерывания на актуализацию страницы и периодически, системными потоками проверки списков.

Обнуление страниц памяти при их освобождении обеспечивается потоком обнуления страниц, переводящем освобожденные страницы в список, из которого происходит их выделение. Этот перевод, формально не одновременный с процедурой освобождения памяти, тем не менее, обеспечивает гарантированное ее обнуление в определенный отрезок времени (зависящий от загрузки системы), даже при отсутствии запросов на выделение памяти (т.е. событием, инициирующим обнуление страницы, является ее освобождение, а не запрос на выделение).

Очистка памяти обеспечивается выборкой доступных страниц памяти из списка обнуленных страниц, а не из всего их множества. Кроме того, распределяемая для объектов память может перезаписываться определенными данными до того момента, когда она будет выделена объекту.

Объектам, хранящимся на диске, предоставляется только то дисковое пространство, которое ими используется. Механизм использования указателей (Read/Write) предотвращает чтение информации за пределами используемой объектами области.

Сопоставление с ФТБ

Функции безопасности «Защита данных пользователя» удовлетворяют следующим функциональным требованиям безопасности:

- FDP_ACC.1 – в ОО реализован механизм дискреционного управления доступом для субъектов – процессов, действующих от имени пользователей, именованных объектов – рабочий стол (Desktop), событие (Event), пара событий (Event pair), порт завершения I/O (I/O Completion Port), задание (Job), ключ реестра (Key), почтовый ящик (Mailslot), именованный канал (Named pipe), каталог NTFS (NTFS directory), файл NTFS (NTFS file), каталог объектов (Object Directory), порт LPC (LPC Port), принтер (Printer), процесс (Process), секция (Section), семафор (Semaphore), символьная ссылка (Symbolic Link), поток (Thread), таймер (Timer), маркеры (Tokens), том (Volume), объект «Window Station», и объект службы каталогов (Active Directory objects) и всех операций между субъектами и объектами;

- FDP_ACF.1 – ФБО обеспечивают доступ к объектам, основываясь на ассоциированных с субъектом идентификаторе, принадлежности к группе (группам) и привилегиях. Описание правил, определяющих порядок доступа к объектам, представлено в алгоритме реализации дискреционного управления доступом;
- FDP_IFC.1 – ФБО осуществляют политику фильтрации информации для субъектов, представляющих пользователей ОО, программ, функционирующих в среде ОО, внешних по отношению к ОО сущностей ИТ, информационного потока, передающегося через ОО и операций перемещения информации;
- FDP_IFF.1 – для осуществления фильтрации информации ФБО используют атрибуты безопасности субъектов доступа и информации. Правила осуществления фильтрации формируются администратором ОО;
- FDP_RIP.2 – ФБО обеспечивают недоступность предыдущего информационного содержания ресурсов при их перераспределении для новых объектов. Данная возможность реализуется через обнуление страниц памяти.

6.1.3 Функции безопасности «Идентификация и аутентификация»

Объект оценки требует, чтобы каждый пользователь был идентифицирован и аутентифицирован до того момента, как от его имени в системе будут выполнены какие-либо действия, и независимо от того выполняет ли он интерактивный доступ к ОО либо осуществляет доступ к ОО через сеть. Единственным исключением является возможность, пользователю завершить работу ОО, не осуществив регистрацию в нем. Однако уполномоченный администратор может запретить данную возможность, если она не удовлетворяет требованиям безопасности.

6.1.3.1 Типы доступа к ОО

Объект оценки поддерживает следующие типы доступа пользователя к ОО:

- интерактивный (Interactive) – локальный доступ пользователя к ОО;
- сетевой (Network) – доступ к ОО через сеть;
- доступ в качестве службы (Batch) – регистрация пользователем процесса в качестве службы;

- доступ в качестве пакетного задания (Service) – доступ пользователя к ОО с помощью средств обработки пакетных заданий;
- разблокировка (Unlock) – тип доступа, имеющий место при разблокировании пользователем рабочей станции;
- удаленно-интерактивный (Remote Interactive) – пользователь выполнил доступ к ОО удаленно посредством службы терминалов либо удаленного рабочего стола.

Интерактивный доступ к ОО предусматривает доступ пользователя к ОО через локальную консоль и предполагает работу пользователя с ОО в интерактивном режиме. Сетевой доступ используется при обращении пользователя к удаленному компьютеру для доступа к его активам. Доступ в качестве пакетного задания предназначен для случаев, когда процессы могут исполняться от имени пользователя без их непосредственного вмешательства, т.е. пользователь получает возможность доступа к ОО с помощью средства обработки пакетных заданий. Доступ в качестве службы используется, когда участники безопасности имеют возможность осуществлять доступ к ОО как службы для установления контекста безопасности. Локальная системная учетная запись всегда сохраняет право доступа к ОО в качестве службы. Любая служба, запускаемая с правами конкретной учетной записи, должна быть наделена правом доступа в качестве службы. По умолчанию эта привилегия не предоставляется никому.

Для каждого из типов доступа к ОО «Интерактивный», «Сетевой», «Доступ в качестве службы» и «Доступ в качестве пакетного задания» определена соответствующая привилегия, которая должна быть предоставлена учетной записи пользователя и группе пользователей с целью возможности контроля доступных пользователю способов доступа к ОО.

6.1.3.2 Регистрация пользователя в ОО

Все запросы на доступ к ОО обрабатываются одним и тем же способом, независимо от их типа (интерактивный, сетевой доступ к ОО, доступ в качестве пакетного задания или в качестве службы). Все они начинаются с предоставления ФБО требуемой информации, такой как имя учетной записи пользователя, пароль и имя домена, в случае, если ОО функционирует в домене.

С целью защиты идентификационной и аутентификационной информации при первоначальном интерактивном доступе пользователя в систему, ОО обеспечивает ее

передачу через доверенный маршрут. Доверенный маршрут вызывается одновременным нажатием комбинации клавиш SAS (Secure Attention Sequence) – Ctrl+Alt+Del, что всегда фиксируется ФБО, т.е. данное действие не может быть прервано или перехвачено недоверенным процессом ОО.

В процессе регистрации пользователя в ОО задействованы процессы Winlogon, LSASS, один или несколько пакетов аутентификации, а также база данных SAM или каталог Active Directory, в случае, если ОО функционирует в домене.

Для получения регистрационных данных от пользователя задействуется служба Winlogon, которая является процессом пользовательского режима, отвечающим за поддержку и управление сеансами интерактивного доступа к ОО. Уведомление о запросе пользователя на регистрацию в ОО служба Winlogon получает при нажатии комбинации клавиш SAS. Затем Winlogon запускает процесс Logonui.exe (сервер пользовательского интерфейса входа в систему), выполняющий загрузку поставщиков учетных данных, настроенных в разделе реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Currentversion\Autentication\Credential Providers. Процесс Logonui.exe может работать с несколькими поставщиками учетных данных одновременно. ОС Windows Vista с Service Pack 1 поставляется с двумя поставщиками учетных данных: интерактивным поставщиком (Authui.dll) и поставщиком смарт-карт (Smart-cardcredentialprovider.dll). Для унификации взаимодействия с пользователем процесс Logonui.exe управляет пользовательским интерфейсом, который видят конечные пользователи.

Служба Winlogon, получив имя и пароль пользователя, передает его в строго определенном формате серверному процессу локальной аутентификации LSASS, который отвечает за получение от службы Winlogon запросов на аутентификацию и вызов пакетов аутентификации для проверки соответствия введенной пользователем аутентификационной информации с той, что храниться в каталоге Active Directory или базе данных SAM.

Модель аутентификации, поддерживаемая в ОО, реализована по модульному принципу на основе пакетов аутентификации (Authentication Packages). Модульность архитектуры позволяет абстрагировать основные системные процедуры аутентификации от конкретных протоколов и реализации. Пакет аутентификации – основной компонент, реализующий логику проверки параметров пользователя и в конечном итоге принимающий решение об успешной или неуспешной регистрации. Пакет

аутентификации представляет собой библиотеку DLL, которая подключается к процессу LSASS при старте ОО. ОО поддерживаются два пакета аутентификации:

- MSV1_0 (\Windows\System32\Msv1_0.dll) – пакет аутентификации, обеспечивающий интерактивную локальную регистрацию пользователя, регистрацию пользователя в отсутствие контроллера домена и поддержку протокола аутентификации NTLM;
- Kerberos (\Wiindows\System32\Kerberos.dll) – пакет аутентификации, реализующий поддержку протокола Kerberos v5, являющегося основным протоколом аутентификации, используемым ОО.

Интерактивная локальная регистрация пользователя в ОО

1. Регистрация пользователя в ОО начинается с момента нажатия им комбинации клавиш SAS (Ctrl+Alt+Del) и явного запроса системой у пользователя его регистрационных данных.

2. После ввода имени и пароля пользователя служба Winlogon передает регистрационные данные в строго определенном формате серверу LSA.

3. Сервер LSA обрабатывает запрос, поочередно вызывая все пакеты аутентификации, зарегистрированные в системе (эти пакеты перечислены в разделе реестра HKLM\SYSTEM\CurrentControlSet\Control\Lsa).

4. Пакет аутентификации MSV1_0 (поскольку этот пакет аутентификации по умолчанию используется для регистрации пользователей на локальных компьютерах) принимает имя пользователя и хэшированную версию пароля и посылает локальному диспетчеру учетных записей безопасности SAM запрос на получение из базы данных SAM информации относительно учетной записи пользователя, включая пароль, членство в группах, в которые входит пользователь, и список ограничений для данной учетной записи. Сначала пакет аутентификации MSV1_0 проверяет существующие ограничения, например разрешенное время или типы доступа. Если ограничения запрещают регистрацию пользователя, пакет аутентификации MSV1_0 возвращает серверу LSA статус отказа.

5. В противном случае, MSV1_0 переходит к этапу сравнения хэшированного пароля и имени пользователя с теми, которые хранятся в базе данных SAM (в случае интерактивной регистрации с кэшированными учетными данными пакет аутентификации MSV1_0 обращается к кэшированной информации через функции LSASS, отвечающие за сохранение и получение информации из базы данных сервера LSA – раздела реестра

HKLM\SECURITY). Если регистрационные данные пользователя совпадают с данными, хранящимися в базе данных SAM, MSV1_0 генерирует LUID-идентификатор сеанса регистрации и создает собственно сеанс регистрации вызовом LSASS. При этом MSV1_0 сопоставляет данный уникальный идентификатор с сеансом и передает данные, необходимые для того, чтобы создать маркер доступа для пользователя.

6. Как только регистрационные данные пользователя аутентифицированы, LSASS ищет в базе данных локальной политики разрешенный пользователю тип доступа. Если тип запрошенного входа в систему не соответствует разрешенному, регистрация прекращается. LSASS удаляет только что созданный сеанс регистрации, освобождая его структуры данных, и сообщает службе Winlogon о неудачной регистрации. Служба Winlogon в свою очередь сообщает об этом пользователю.

7. Если же запрошенный тип входа в систему разрешается, LSASS генерирует маркер доступа, определяющий контекст безопасности пользователя, добавляя в него любые дополнительные идентификаторы безопасности (например, Everyone, Interactive и т.п.) и включая все привилегии, назначенные всем идентификаторам, содержащимся в маркере доступа данного пользователя.

8. После успешного создания маркера доступа LSASS дублирует его и передает службе Winlogon.

9. Далее служба Winlogon просматривает параметр реестра `HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\Userinit` и создает процесс для запуска программ, указанных в строковом значении этого параметра. Значение этого параметра по умолчанию приводит к запуску Userinit.exe, который загружает профиль пользователя, а затем создает процесс для запуска программ, перечисленных в `HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\Shell` (значением этого параметра по умолчанию является Explorer.exe).

Регистрации пользователя в домене

Базовая последовательность действий при использовании пакета аутентификации Kerberos в основном та же, что и в случае с MSV1_0. Однако в большинстве случаев доменная регистрация проходит на рабочих станциях или серверах, входящих в домен (а

не на контроллере домена), поэтому пакет аутентификации в процессе проверки подлинности должен взаимодействовать со службой Kerberos на контроллере домена.

Получив запрос на доступ к ОО, сервер LSA передает его в формате пакета аутентификации Kerberos службе Kerberos на контроллере домена, сообщая ей имя пользователя, имя домена и преобразованную с использованием хэшированного пароля пользователя строку, содержащую текущее системное время (запрос на получение билета TGT).

Получив запрос на аутентификацию, служба Authentication Service (AS) использует хэшированный пароль для указанной учетной записи из каталога Active Directory и осуществляет обратное преобразование присланной клиентом строки. Если операция завершена успешно, а время, значащееся в строке, не выходит за рамки, определяемые параметром «Максимальная погрешность синхронизации часов компьютера» политики Kerberos, то служба AS успешно аутентифицирует пользователя, осуществляющего регистрацию в домене.

После проверки информации об имени и пароле пользователя с помощью объектов учетных записей пользователей (user account objects) Active Directory служба Kerberos инициирует AS-ответ, содержащий билет TGT (Ticket-Granting Ticket – «билет на выдачу билета») и отсылает его клиенту. В составе билета TGT включен идентификатор безопасности учетной записи и всех групп, в которые входит данный пользователь. Эта информация нужна службе TGS для создания новых билетов, которые предоставили бы пользователю право использовать другие службы не только на его локальном компьютере, но и на других компьютерах сети. Таким образом, успешная аутентификация пользователя в домене не означает, что пользователь получает разрешение на доступ к защищаемым сетевым ресурсам.

Чтобы получить доступ к защищаемым ресурсам клиент посылает службе Ticket Granting Service (TGS) запрос, содержащий полученный билет TGT. Служба Kerberos генерирует и посылает ответ от службы Ticket Granting Service. Он содержит сессионный билет (session ticket). В данном билете содержатся идентификатор безопасности учетной записи и всех глобальных групп, скопированных службой Kerberos с оригинального билета TGT. На основании этого билета сервер, содержащий защищаемые активы, аутентифицирует пользователя и формирует для него маркер доступа

Главным компонентом службы Kerberos является центр распределения ключей KDC (Key Distribution Center), функционирующий как доменная служба на контроллере

домена (ОО). В соответствии со спецификацией Kerberos центр распределения ключей KDC исполняется как единый процесс, обеспечивающий две службы:

- Authentication Service (AS) — служба, выдающая билеты Ticket-Granting Ticket (TGT) аутентифицированным клиентам. Этот билет выдается пользователям, которые успешно прошли первоначальную регистрацию;
- Ticket Granting Service (TGS) — служба, выдающая Session Tickets, — сеансовые билеты. Чтобы получить доступ к какому-либо сетевому активу, пользователь должен запросить сеансовый билет для этого сервера у службы TGS. При этом необходимо предъявить службе TGS свой полученный ранее от службы AS билет TGT. Затем сеансовый билет, полученный от TGS, предъявляется требуемому серверу.

Служба KDC всегда располагается на контроллере домена. Обе службы, функционирующие в рамках KDC, запускаются сервером локальной аутентификации LSA контроллера и исполняются в рамках процесса LSA. Ни одна из служб KDC не может быть остановлена или отключена. Фактически понятие контроллер домена взаимно однозначно определяется наличием работающих на сервере служб Authentication Service и Ticket Granting Service. Если в домене несколько контроллеров, столько же в нем будет и KDC. Все контроллеры домена могут принимать запросы пользователей и выдавать билеты.

В качестве защищенного хранилища учетных записей ОО использует каталог Active Directory. Каждая учетная запись представлена в виде объекта с определенным набором атрибутов. Для служб аутентификации наибольшую важность представляет атрибут, хранящий пароль пользователя, точнее, не сам пароль, а полученный на его основе ключ, используемый для преобразования данных, передаваемых в рамках сеанса пользователя со службой AS: при запросе и получении билета TGT.

Между двумя механизмами аутентификации (по протоколу Kerberos и NTLM) существуют два основных отличия. Первое заключается в том, что запрос NTLM, содержащий имя пользователя и пароль в хэшированном виде, пересылается локальными ФБО на сервер. Сервер сравнивает представленный в хэшированном виде пароль с версией, хранящейся в базе данных. Если пароли совпадают, аутентификация считается успешной. В случае локальной аутентификации пароли не хэшируются и серверу не передаются, пароль сравнивается с хранящимся в локальной базе данных экземпляром. Kerberos, напротив, требует, чтобы запрос на доступ был частично преобразован с

помощью хэшированного пароля. Преобразованный запрос пересылается соответствующему контроллеру домена, который в свою очередь ищет хешированный пароль пользователя в своей базе данных. Далее данный пароль используется для обратного преобразования запроса на вход. Если операция обратного преобразования выполнена успешно и запрос на вход содержит соответствующие временные метки (т.е. определен в рамках временного периода, установленного администратором), аутентификация считается успешной.

Второе отличие заключается в том, как осуществляются последующее обращение к удаленным ресурсам. В случае NTLM при обращении к удаленным ресурсам пользователь должен проходить процедуру входа в ОС удаленного компьютера. По существу данный процесс представляет сетевой доступ и будет следовать тому же алгоритму как при интерактивной локальной регистрации. В случае Kerberos, для того, чтобы взаимодействовать с сетевым сервером, необходимо пройти дополнительную аутентификацию уже на самом сервере. Поскольку пользователь ранее был опознан службами аутентификации, нет необходимости снова просить его ввести свои регистрационные параметры. Таким образом, чтобы получить доступ к ресурсам на сетевом сервере, он должен запросить сеансовый билет для этого сервера у службы Ticket Granting Service (TGS). При этом необходимо предъявить службе TGS свой полученный ранее от службы AS билет TGT. Затем сеансовый билет, полученный от TGS, предъявляется нужному серверу, на основании этого ресурсный сервер аутентифицирует пользователя и формирует маркер доступа.

6.1.3.3 База данных атрибутов пользователя

Объект оценки поддерживает базу данных, в которой полностью определены учетные записи пользователей и групп безопасности. При этом хранение учетных записей пользователей и групп, определенных на локальном компьютере, осуществляется в базе данных диспетчера учетных записей безопасности SAM (Security Account Manager), а доменных учетных записей пользователей, групп и компьютеров в каталоге Active Directory на контролерах домена.

Каждая учетная запись представлена в базе данных следующим минимальным набором атрибутов:

– *имя учетной записи* - используется для представления учетной записи в удобочитаемой форме;

- *идентификатор безопасности SID* – идентификатор, используемый для однозначного представления учетной записи пользователя или группы в рамках ОО;
- *пароль* – используется только для учетных записей пользователей. Основная задача заключается в аутентификации учетной записи пользователя при его входе в ОО;
- *принадлежность к группе* – используется, чтобы связать членов группы (учетные записи пользователей или других групп) с единой учетной записью;
- *привилегии* – используются для связывания привилегий ФБО с учетной записью;
- *права на доступ к системе* – право, присвоенное пользователю и определяющее способы его доступа к системе;
- *управляющая информация* – используется, чтобы контролировать дополнительные относящиеся к безопасности параметры учетных записей, таких как время действия учетной записи, факт блокировки, срок действия пароля, историю паролей и время последнего изменения пароля;
- *другая информация, не относящаяся к безопасности,* – используется для дополнительного описания учетной записи, например, действительное имя и предназначение учетной записи.

Действительная совокупность всех атрибутов учетных записей пользователей и групп безопасности зависит от среды функционирования ОО.

6.1.3.4 Политики учетных записей

Политики учетных записей определяют взаимодействие учетных записей пользователей с компьютерами или доменами. Политики учетных записей определяются и управляются уполномоченным администратором. Через политики учетных записей можно задать политику паролей, политику блокировки учетной записи и политику Kerberos.

Политика паролей

С использованием политики паролей определяется следующие параметры паролей:

- *максимальный срок действия пароля* – определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем ОО потребует от пользователя заменить его. Значение для данного параметра может быть

определено в диапазоне от 1 до 999 дней. Установив число дней равным 0, можно снять всякие ограничения срока действия пароля;

- *минимальная длина пароля* – определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Установив число символов равным 0 можно отменить использование пароля;
- *минимальный срок действия пароля* – определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Значение для данного параметра может быть определено в диапазоне от 1 до 998 дней. Установив число дней равным 0 можно разрешить немедленное изменение пароля пользователем. Минимальный срок действия пароля должен быть меньше, чем максимальный срок действия пароля, если только не задан неограниченный срок действия пароле установкой значения 0;
- *пароль должен отвечать требованиям сложности* – данное требование определяет, должны ли пароли отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:
  - пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
  - пароль должен состоять не менее чем из шести символов;
  - в пароле должны присутствовать символы как минимум трех категорий из числа следующих:
    - прописные буквы английского алфавита (от A до Z);
    - строчные буквы английского алфавита (от a до z);
    - десятичные цифры (от 0 до 9);
    - специальные символы (например, !, $, #, %), символы из расширенного набора ASCII, символические или лингвистические знаки.
- *хранить пароли, используя обратимое преобразование* – определяет, использует ли ОО обратимое преобразование для хранения паролей. Использование данного параметра позволяет обеспечить поддержку

приложений, использующих протоколы, которым для проверки подлинности необходимо знать пароль пользователя.

Политика блокировки учетной записи

Политика блокировки учетной записи определяет условия и период времени блокировки учетной записи и позволяет задать:

- *временной интервал блокировки учетной записи* – определяет число минут, в течение которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Значение для данного параметра может быть определено в диапазоне от 1 до 99 999 минут. Если установить значение 0, учетная запись будет блокирована на все время до тех пор, пока администратор не разблокирует ее явным образом;
- *пороговое значение блокировки* – определяет число неудачных попыток доступа к ОО, после которых учетная запись пользователя блокируется. Значение для данного параметра может быть определено в диапазоне от 1 до 999. Установив число равным 0 можно запретить разблокировку данной учетной записи;
- *временной интервал, после которого произойдет сброс счетчика блокировки* – определяет число минут, которые должны пройти после неудачной попытки доступа к ОО, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше временного интервала блокировки учетной записи.

6.1.3.5 Стойкость аутентификации

Объект оценки предоставляет набор функций, позволяющих управлять политиками учетных записей. Данные функции обеспечивают возможность задания параметров политики учетных записей, в том числе минимальную длину пароля. Рекомендуется, чтобы минимальная длина пароля превышала восемь символов (при использовании множества из 90 символов количество возможных вариантов пароля превысит $4{,}3 \times 10^{15}$). Пароли могут содержать до 127 символов, однако максимальное количество значимых символов в паролях, используемых для аутентификации субъектов доступа в ОО, составляет 14.

Сопоставление с ФТБ

Функции безопасности «Идентификация и аутентификация» удовлетворяют следующим функциональным требованиям безопасности:

- FIA_AFL.1 – ФБО обнаруживают, когда происходит установленное администратором ОС число (50) неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя, при достижении установленного числа неуспешных попыток аутентификации функции безопасности среды ИТ осуществляют блокировку регистрационной записи пользователя ОО на 15 минут;
- FIA_ATD.1 – ФБО поддерживают базу данных атрибутов пользователей, в которой полностью определены учетные записи пользователей. Каждая учетная запись представлена в данной базе набором атрибутов: идентификатором безопасности, принадлежностью к группе, привилегиями, правами доступа к ОО, а также другой информацией;
- FIA_SOS.1 – ФБО предоставляют механизм для верификации качества паролей на доступ к ОО;
- FIA_UAU.2 – ФБО обеспечивают аутентификацию до любых действий субъектов доступа к ОО;
- FIA_UAU.7 – с целью предотвращения раскрытия пароля субъекта доступа во время интерактивной аутентификации ФБО обеспечивают отображение вводимого пароля в виде символов «*»;
- FIA_UID.2 – ФБО осуществляют идентификацию субъектов доступа к ОО до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого субъекта доступа;
- FIA_USB.1 – каждый процесс или поток имеет ассоциированный с ним маркер доступа, обеспечивающий надежную ассоциацию атрибутов безопасности пользователя, определенных в маркере доступа, с субъектами, действующими от имени пользователя;
- FTA_TSE.1 – по истечению срока действия пароля ФБО не предоставят пользователю доступ в ОО до тех пор, пока он не будет изменен;
- FTP_TRP.1 – ФБО обеспечивают защищенный от подмены механизм запроса на доступ к ОО (нажатие комбинации клавиш Ctrl-Alt-Del), который обеспечивает

прямое взаимодействие пользователя с ФБО с целью передачи регистрационной информации и интерактивного доступа к ОО;

– FMT_SMR.3 – чтобы принять роль уполномоченного администратора, пользователь должен подтвердить полномочия в окне средства «Контроль учетных записей пользователей (UAC)».

6.1.4 Функции безопасности «Управление безопасностью»

Объект оценки поддерживает ролевую модель и предоставляет определенный набор функций управления различными политиками и характеристиками безопасности.

6.1.4.1 Роли

Представление ролей в рамках ОО реализовано через механизм назначения учетной записи пользователя определенных привилегий или включение ее в состав участников группы. При осуществлении доступа к ОО, пользователю присваивается определенная роль, для которой определено членство в группах и установлены привилегии. Несмотря на то, что в ОО могут быть определены различные роли, в ЗБ рассматриваются две логические роли: уполномоченного администратора ОО и пользователя ОО.

Роль уполномоченного администратора ОО может быть представлена любой учетной записью, для которой назначены соответствующие привилегии (например, право смены владельца файлов или других объектов). Вторым вариантом является добавление данной учетной записи в одну из нескольких предустановленных административных групп, например, локальную группу безопасности «Администраторы». Пользователю будут предоставлены полномочия администратора, только в том случае, если он зарегистрируется под той учетной записью, для которой определены соответствующие привилегии, или, которая является членом соответствующей административной группы.

6.1.4.2 Функции управления безопасностью

Объект оценки поддерживает набор политик и характеристик безопасности, которые требуют соответствующего управления. За некоторым исключением, функции по управлению безопасностью предоставлены только уполномоченному администратору ОО. Данное ограничение реализуется через использование привилегий и механизм управления

доступом. ОО поддерживает функции управления безопасностью для следующих политик и характеристик безопасности:

Политика аудита – функции управления политикой аудита предоставляют уполномоченным администраторам ОО возможность разрешать или запрещать аудит событий, выполнять настройку категорий событий, которые будут подвергнуты аудиту, указывать тип контролируемого события (успех/отказ), управлять (создание, удаление и очистка) журналом безопасности и его характеристиками (размер, режимом очистки), а также определять реакцию ОО в случае невозможности ведения аудита событий безопасности. Уполномоченный администратор может также указать для конкретного объекта ОО, какие пользователи и какие права доступа к данному объекту будут контролироваться.

Политика учетных записей – функции управления политикой учетных записей предоставляют уполномоченным администраторам ОО возможность устанавливать ограничения на применяемые пароли и определять параметры блокировки учетных записей. Определяя политику использования паролей, уполномоченный администратор ОО задает минимальную длину пароля, требование неповторяемости паролей, минимальный и максимальный срок действия пароля. В случае превышения максимального срока действия пароля, пользователь не сможет осуществить доступ к ОО до того момента, пока не сменит пароль. Параметры блокировки учетных записей определяют пороговое значение неуспешных попыток доступа к ОО, при превышении которого учетная запись будет заблокирована, продолжительность блокировки и интервал времени, после которого произойдет сброс счетчика блокировки.

Политика управления базой данных учетных записей пользователей – функции управления базой данных учетных записей позволяют уполномоченному администратору управлять (определять, назначать и удалять) атрибутами безопасности учетных записей пользователей и групп. Каждая учетная запись описывается следующим минимальным набором атрибутов: имя учетной записи, идентификатор безопасности, пароль, членство в группах и другая информация, относящаяся и не относящаяся к безопасности. Из всего представленного набора атрибутов безопасности пользователю разрешено изменять только собственный пароль. Уполномоченный администратор при создании учетной записи пользователя определяет только начальный пароль, который в последствии может быть изменен как самим администратором, так и самостоятельно пользователем. При изменении значения пароля на новое, обязательным требованием

является знание старого пароля, которое необходимо указать при выполнении данной процедуры.

Политика назначения прав пользователя – функции управления назначением прав пользователя позволяют уполномоченному администратору назначать или удалять для конкретных учетных записей пользователей или групп права доступа к ОО и определенные привилегии.

Политика управления дисковыми квотами – функции управления дисковыми квотами позволяют уполномоченному администратору управлять дисковыми квотами на томах файловой системы. Уполномоченный администратор ОО имеет возможность включать или отключать использование дисковых квот, определять размер дисковых квот, устанавливаемых по умолчанию, а также задавать требуемое действие при превышении пользователя выделенного объема квот.

Политика управления очисткой памяти – функции управления механизмами очистки памяти позволяют уполномоченному администратору ОО включать и выключать режим очистки содержимого страничного файла подкачки.

Политика управления приоритетами процессов – функции управления приоритетами процессов позволяют уполномоченному администратору ОО назначать приоритеты процессам на использование процессорного ресурса.

Политика управления тестированием оборудования и ФБО – функции управления тестированием оборудования и ФБО позволяют уполномоченному администратору определять условия тестирования.

Сопоставление с ФТБ

Функции безопасности «Управление безопасностью» удовлетворяют следующим функциональным требованиям безопасности:

- FMT_MOF.1– ФБО предоставляют возможность выполнять определенные действия над функциями из числа ФБО в части управляемых характеристик безопасности только уполномоченным администраторам безопасности, перечень действий, функций и управляемых характеристик приведен в таблице 5.3;
- FMT_MSA.1– возможность изменять политику дискреционного управления доступом контролируется посредством полномочий на изменение списков дискреционного управления доступом;

- FMT_MSA.3 – ФБО обеспечивают применение устанавливаемых по умолчанию прав доступа ко всем создаваемым объектам. При создании новых объектов для них определяется соответствующий дискреционный список управления доступом. Пользователи, создающие объекты, могут специфицировать дескриптор безопасности, содержащий список DACL, чтобы переопределить значения, принятые по умолчанию;
- FMT_MTD.1 (1) – ФБО предоставляют возможность создавать, удалять или очищать журнал аудита событий безопасности только уполномоченному администратору ОО;
- FMT_MTD.1 (2) – ФБО предоставляют возможность доступа к журналу аудита событий безопасности только уполномоченному администратору ОО;
- FMT_MTD.1 (3) – ФБО предоставляют возможность модификации атрибутов безопасности пользователя (за исключением пароля, который может быть самостоятельно изменен пользователем), только уполномоченному;
- FMT_MTD.1 (4) – ФБО предоставляют возможность устанавливать начальный пароль для пользователя только уполномоченному администратору ОО;
- FMT_MTD.1 (5) – ФБО предоставляют возможность изменять начальный пароль для пользователя только уполномоченному администратору ОО или уполномоченному пользователю;
- FMT_MTD.1 (6) – ФБО предоставляют возможность изменять интервал продолжительности блокировки учетной записи только уполномоченному администратору ОО;
- FMT_MTD.1 (7) – ФБО предоставляют возможность изменять минимальную длину пароля только уполномоченному администратору ОО;
- FMT_MTD.2 – ФБО предоставляют уполномоченному администратору ОО возможность определять пороговое значение количества неуспешных попыток аутентификации, при превышении установленного порогового значения ФБО должны блокировать учетную запись пользователя на время, определенное администратором ОО;
- FMT_REV.1 (1) – ФБО предоставляют возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО, администраторами ОО и объектами, только уполномоченному администратору ОО и осуществляют

правила отмены полномочий у пользователей ОО и администраторов ОО на доступ к объектам, а также правила отмены прав доступа к объекту (модификацию списка дискреционного доступа);

- FMT_REV.1 (2) – ФБО предоставляют возможность отмены атрибутов безопасности, ассоциированных с объектами, только пользователю ОО, уполномоченному согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта, и осуществляют правила отмены прав доступа к объекту (модификацию списка дискреционного доступа);
- FMT_SAE.1 – ФБО предоставляют возможность назначать срок действия аутентификационных данных только уполномоченному администратору ОО, ФБО осуществляют блокирование ассоциированной с пользователем учетной записи по истечении срока действия аутентификационных данных;
- FMT_SMR.1 – ФБО поддерживают ролевую модель, определяя роль администратора ОО и пользователя ОО.

6.1.5 Функции безопасности «Защита ФБО»

Функции безопасности ОО «Защита ФБО» обеспечивают:

- целостность системы;
- доступ к объекту посредством описателей;
- разделение доменов;
- службу времени.

6.1.5.1 Целостность системы

Аппаратная платформа, обеспечивающая функционирование ОО, была протестирована с целью определения поддержки функций безопасности. Тесты были направлены на определение правильности функционирования системной платы, а также периферийных устройств, таких как модули памяти, жесткий магнитный диск, видеоадаптер, порты I/O. Данные тесты были разработаны, чтобы убедиться в корректной реализации тех возможностей, которые положены в основы функций безопасности (например, обработка прерываний, управление памятью, управление заданиями и т.д.).

6.1.5.2 Посредничество при доступе к объекту

Механизм доступа к объекту в большинстве случаев основан на использовании описателей объектов. Получение описателя обычно происходит при открытии или создании объекта. В этих случаях, ФБО обеспечивают подтверждение доступа перед созданием нового описателя для субъекта. Описатели могут быть также унаследованы от родительских процессов или напрямую скопированы (при наличии соответствующих прав доступа) у другого субъекта. В любом случае, перед созданием описателя, ФБО обеспечивают проверку политики безопасности на предмет возможности владения (и таким образом, возможности доступа) субъектом описателем объекта. Описатель всегда имеет маску назначенного доступа, ассоциированную с ним. Данная маска доступа определяет, какие права доступа к объекту будут предоставлены субъекту согласно установленной политики безопасности. ФБО обеспечивают требуемый доступ согласно маске назначенного доступа описателя при каждой попытки его использования. В некоторых случаях, таких как взаимодействие со службой каталога, доступ к объектам осуществляется напрямую по имени без промежуточного этапа получения описателя объекта.

6.1.5.3 Разделение доменов

Объект оценки обеспечивает изоляцию процессов и поддерживает домен безопасности для собственного безопасного выполнения. Домены безопасности состоят из следующих компонентов:

- аппаратных средств;
- программного обеспечения режима ядра;
- доверенных процессов пользовательского режима;
- инструментальных средств администрирования процессов пользовательского режима.

Управление аппаратными средствами ФБО осуществляется программным обеспечением ФБО режима ядра. Аппаратные средства ФБО не могут быть модифицированы недоверенными субъектами. Защита программного обеспечения ФБО режима ядра от модификации обеспечивается посредством контроля состояния функционирования аппаратных средств и защитой памяти. Аппаратные средства ФБО обеспечивают инструкции, генерирующие программные прерывания, позволяющие переходить из состояния режима пользователя в состояние режима ядра. Программное

обеспечение ФБО режима ядра осуществляет обработку всех прерываний и определяет обоснованность сделанных вызовов в режиме ядра. Механизм защиты памяти реализован таким образом, что напрямую обращаться к памяти могут только компоненты в режиме ядра. Прямое взаимодействие с памятью внешних подсистем и приложений пользовательского режима невозможно.

ФБО обеспечивают изоляцию всех процессов пользовательского режима посредством контекста выполнения, контекста безопасности и ограничения выделенного им адресного пространства (использование механизма виртуального адресного пространства). Структура данных, определяемая адресным пространством процесса, контекстом выполнения и контекстом безопасности, хранится в защищенной памяти режима ядра.

Инструментальные средства администрирования реализуют функции управления в контексте безопасности процесса, запущенного от имени уполномоченного администратора ОО. Процессы, выполняемые в контексте учетной записи администратора ОО, защищены таким же образом, как и другие процессы пользовательского режима, т.е. через изоляцию посредством виртуального адресного пространства.

Пользовательские процессы, по аналогии с процессами ФБО, также исполняются в собственном виртуальном адресном пространстве, что, собственно, обеспечивает их защищенность друг от друга.

6.1.5.4 Служба времени

Поддерживаемая ОО аппаратная платформа включает контроллер часов реального времени, представляющий устройство, доступ к которому может быть возможен только через функции, предоставляемые ФБО. В частности, ФБО обеспечивают функции, которые позволяют пользователям, включая сами ФБО, запрашивать и устанавливать время, а также возможность синхронизации времени с внешним источником времени. Возможность запроса времени ни чем не ограничена, в то время как изменение системного времени требует полномочий на выполнение данной операции. Данная привилегия предоставлена только уполномоченным администраторам ОО с целью обеспечения непротиворечивости службы времени.

Сопоставление с ФТБ

Функции безопасности «Защита ФБО» удовлетворяют следующим функциональным требованиям безопасности:

- FPT_ATM.1 – ФБО осуществляет тестирование среды-ИТ функционирования (аппаратной части), критичной по безопасности, в процессе загрузки ОО и по требованию уполномоченного администратора ОО;
- FPT_RVM.1 – ФБО обеспечивают, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ;
- FPT_RCV.1 – ФБО предоставляют возможность и средства для уполномоченного администратора, позволяющие осуществить возврат ОО в безопасное состояние в случае сбоя или прерывания обслуживания;
- FPT_SEP.1 – ФБО обеспечивают поддержание домена безопасности для собственного выполнения, защищающего их от вмешательства и искажения недоверенными субъектами;
- FPT_STM.1 – контроллер часов реального времени, реализованный на поддерживаемой ОО аппаратной платформе, в сочетании с периодической синхронизацией с внешним источником времени и возможностью их изменения только уполномоченным администратором ОО, предоставляют надежные метки времени для ФБО;
- FPT_TST.1 – ФБО осуществляют самотестирование в процессе запуска ОО и по требованию уполномоченного пользователя в процессе функционирования;
- FPT_ITC.1 – ФБО обеспечивают конфиденциальность передаваемой для аутентификации и авторизации на контроллере домена аутентификационной информации путем хеширования.

6.1.6 Функции безопасности ОО «Использование ресурсов ОО»

Объект оценки предоставляет возможность ограничивать на определенном томе NTFS объем доступного для пользователя дискового пространства. Любой том NTFS обладает набором свойств, включая информацию об используемых дисковых квотах, которые могут быть изменены только уполномоченным администратором. Эти свойства позволяют ему разрешать или запрещать использование дисковых квот на выбранном

томе, указывать размер квоты, выделяемой по умолчанию, задавать порог выдачи предупреждений и определять действие при превышении квоты.

Дисковые квоты применяются только к томам и не зависят ни от структуры папок на томах, ни от схемы размещения томов на физических дисках. Если один физический диск содержит несколько томов, и квоты применяются к каждому тому, то каждая квота применяется только к указанному тому. Если один том занимает несколько физических дисков, то ко всему составному тому применяется одна квота.

Уполномоченные администраторы могут настроить ОО таким образом, чтобы:

- запретить использование дискового пространства сверх указанного предела и регистрировать случаи превышения этого предела пользователями ОО;
- регистрировать события превышения пользователями ОО указанного порога предупреждения, то есть отметки, при прохождении которой пользователь ОО приближается к заданному для него пределу использования дискового пространства.

Предельный размер выделяемой квоты и порог предупреждений могут быть установлены для каждой учетной записи по отдельности. Все остальные параметры применяются для всех пользователей данного тома.

Используемое дисковое пространство ассоциируется с учетной записью пользователя ОО, «владеющего» им, на основе атрибута объекта, определяющего его владельца. При первом создании пользователем объекта на томе с разрешенным квотированием для его учетной записи создается запись квоты (если она не была создана явным образом). Эта запись квоты изначально задает дисковое пространство, выделяемое по умолчанию, определяет порог выдачи предупреждений и в дальнейшем используется для управления дисковым пространством, установленным для учетной записи пользователя. Каждый раз, когда для данной учетной записи необходимо выделить дисковое пространство (например, при создании или изменении объекта), проверяется размер выделенной квоты, порог предупреждений и происходит изменение записи квоты для этой учетной записи. При превышении порога выдачи предупреждений или установленного размера выделенных квот, выполняются определенные уполномоченным администратором ОО действия.

Для организации использования процессорного ресурса и выделяемых системных ресурсов администраторам ОО предоставляется механизм установления приоритетов выполняемым процессам.

Сопоставление с ФТБ

Функции безопасности ОО «Использование ресурсов ОО» удовлетворяют следующим функциональным требованиям безопасности:

- FRU_PRS.1 – ФБО дают возможность установить приоритет каждому процессу и обеспечивают доступ к процессорному ресурсу на основе приоритетов;
- FRU_RSA.1 – Механизм квотирования на томах файловой системы предоставляет уполномоченному администратору ОО возможность эффективно ограничивать общий объем дискового пространства, которое доступно для пользователя ОО или группы пользователей.

6.1.7 Функции безопасности ОО «Блокирование сеанса»

Объект оценки предоставляют пользователям ОО возможность блокировать собственный интерактивный сеанс немедленно или по истечении определенного ими временного интервала. После того, как пользователь ОО осуществил доступ к ОО, он может заблокировать сеанс путем нажатия комбинации клавиш Ctrl-Alt-Del. Данная комбинация клавиш гарантированно фиксируется ФБО и не может быть перехвачена или изменена каким-либо пользовательским процессом. Результатом нажатия данной комбинации клавиш является появление диалогового окна, содержащего меню функций, одна из которых предназначена для блокирования сеанса пользователя ОО.

С другой стороны, пользователи ОО могут блокировать собственный сеанс после настройки через свойства экрана режима заставки.

Пользователь ОО может использовать в качестве заставки какую-либо программу, определять время неактивности, по истечению которого включится режим заставки, и задавать пароль, необходимый для возврата в сеанс пользователя ОО. ФБО непрерывно контролируют активность мыши и клавиатуры и, если они бездействуют в течение установленного пользователем ОО времени, ФБО инициируют режим заставки и блокируют сеанс пользователя ОО.

При блокировании сеанса вручную либо после каких-либо манипуляций мышью или нажатия клавиатуры в режиме заставки (предполагается, что для выхода из режима заставки требуется пароль, в противном случае произойдет немедленный возврат в сеанс), ФБО отобразят диалоговое окно входа, сообщающее о том, что пользователю ОО необходимо нажать комбинацию клавиш Ctrl-Alt-Del для повторного доступа к ОО.

Независимо от того, как был заблокирован сеанс, пользователь ОО должен нажать комбинацию клавиш Ctrl-Alt-Del для вызова диалогового окна аутентификации. Далее пользователь ОО должен заново ввести пароль, который был кэширован при первоначальной регистрации, и, в случае ввода корректного пароля, пользователь ОО возобновляет собственный сеанс.

Объект оценки предоставляет уполномоченному администратору ОО возможность ввода собственного идентификатора и пароля для доступа к ОО. Если ФБО успешно аутентифицируют уполномоченного администратора ОО, сеанс пользователя, уже выполнившего первоначальную регистрацию в ОО, будет завершен. Для администратора ОО будет создан новый сеанс.

Сопоставление с ФТБ

Функции безопасности ОО «Блокирование сеанса» удовлетворяют следующим функциональным требованиям безопасности:

- FTA_SSL.1 – ОО позволяет пользователю ОО и уполномоченному администратору ОО определять период бездействия, по окончании которого сеанс будет заблокирован. Для возврата в собственный сеанс пользователь ОО или администратор ОО должен осуществить повторную процедуру аутентификации;
- FTA_SSL.2 – ОО предоставляет пользователю ОО и уполномоченному администратору ОО возможность самостоятельно блокировать собственный сеанс. Для возврата в собственный сеанс пользователь ОО или уполномоченный администратор ОО должен осуществить повторную процедуру аутентификации.

6.2 Меры доверия к безопасности ОО

Для удовлетворения требований доверия к безопасности согласно ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), применены следующие меры доверия к безопасности ОО:

- управление конфигурацией;
- предоставление руководств;

– предоставление проектной документации;
– тестирование;
– оценка стойкости функций безопасности.

6.2.1 Управление конфигурацией

Меры управления конфигурацией, применяемые корпорацией Microsoft®, обеспечивают уникальную идентификацию версий ОО.

Корпорация Microsoft осуществляет уникальную маркировку ОО, позволяющую отличать разные версии ОО. Это достигается маркированием упаковки, носителей. Кроме того, ОО может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку или графический интерфейс.

Корпорация Microsoft использует многократную маркировку ОО – к названию и номеру версии добавляются номера пакетов исправлений и пакетов обновлений; при этом применяемые корпорацией Microsoft меры управления конфигурацией обеспечивают согласованность меток вследствие непересечения областей значения меток.

Корпорация Microsoft применяет меры управления конфигурацией, связывающие маркированные руководства, поставляемые в составе ОО, с данным ОО.

Сопоставление с ТДБ

Меры доверия, связанные с управлением конфигурацией, удовлетворяют следующему требованию доверия:

– ACM_CAP.1.

6.2.2 Представление руководств

Заявитель предоставляет руководство безопасной установки, генерации и запуска, разработанное корпорацией Microsoft®. В процедурах установки, генерации и запуска описаны шаги, необходимые для получения безопасной конфигурации ОО, описанной в ЗБ. Эти процедуры задокументированы в «Windows Vista с Service Pack 1 Security Guide»

Заявитель предоставляет руководства администратора и пользователя, в которых описываются действия по выполнению функций безопасности ОО и приводятся предупреждения уполномоченным администраторам и пользователям о действиях, которые могут скомпрометировать безопасность ОО. Эти руководства задокументированы в «Windows Vista с Service Pack 1 Security Guide»

Сопоставление с ТДБ

Меры доверия, связанные с представлением руководств, удовлетворяют следующим требованиям доверия:

– ADO_IGS.1;
– AGD_ADM.1;
– AGD_USR.1.

6.2.3 Представление проектной документации

Проектная документация ОО, предоставляемая на оценку, включает функциональную спецификацию. Функциональная спецификация является неформальной.

В функциональной спецификации определены все внешние (то есть, видимые для пользователя или администратора) интерфейсы функций безопасности ОО, описаны режимы функционирования ОО на каждом внешнем интерфейсе, включая описание результатов, нештатных ситуаций и сообщений об ошибках.

Материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией направлены на отображения соответствия функций безопасности, представленных в функциональной спецификации, функциям безопасности, идентифицированным в краткой спецификации.

Сопоставление с ТДБ

Меры доверия, связанные с представлением проектной документации, удовлетворяют следующим требованиям доверия:

– ADV_FSP.1;
– ADV_RCR.1.

6.2.4 Тестирование

Заявитель предоставляет ОО, пригодный для тестирования, с соответствующей документацией, это позволяет провести независимое тестирование ФБО и сделать заключение, выполняются ли ФБО в соответствии со спецификациями.

Сопоставление с ТДБ

Меры доверия, связанные с тестированием, удовлетворяют требованию доверия:

– ATE_IND.1.

6.2.5 Оценка стойкости функций безопасности

Для механизма парольной защиты, являющегося вероятностным, предоставляется материал анализа стойкости функции безопасности (аутентификации). Анализ стойкости функции безопасности представлен в документе «Операционная система Windows Vista с Service Pack 1. Свидетельство анализа стойкости функций безопасности ОО. Версия 1.0, 2007, MS.Win_Vista.СФБ».

Сопоставление с ТДБ

Меры доверия, связанные с оценкой стойкости функций безопасности, удовлетворяют следующему требованию доверия:

– AVA_SOF.1.

7. Утверждения о соответствии ПЗ

В данном разделе излагается утверждение о соответствии ОО конкретному профилю защиты и приводится обоснование этих утверждений.

7.1 Ссылка на ПЗ

Объект оценки соответствует профилю защиты ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

7.2 Конкретизация ПЗ

Все требования безопасности, сформулированные в ПЗ ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Эти операции завершены в настоящем ЗБ в полном объеме (см. таблицу 7.1 – компоненты требований с пометкой «завершено»).

Кроме того, исходя из особенностей рассматриваемого ОО, по отношению к ряду функциональных требований, взятых из ПЗ, в настоящем ЗБ была применена операция уточнения (см. таблицу 7.1 – компоненты требований с пометкой «уточнено»).

Функциональные требования, операции над которыми были завершены, а также требования, уточненные в ЗБ относительно ПЗ, приведены в таблице 7.1.

Таблица 7.1 – Конкретизация функциональных требований по отношению к ПЗ ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003»

Наименование требования	Изменение
FAU_GEN.1	уточнено
FAU_SAR.3	завершено
FAU_SEL.1	завершено
FAU_STG.3	завершено
FAU_STG.4	завершено
FDP_ACC.1	завершено
FDP_ACF.1	завершено уточнено
FIA_AFL.1	завершено
FIA_ATD.1	завершено
FIA_SOS.1	завершено
FIA_USB.1	завершено
FMT_MOF.1	завершено
FMT_MSA.1	завершено
FMT_MSA.3	завершено
FMT_REV.1	завершено
FMT_SAE.1	завершено
FMT_SMR.1	завершено
FTA_TSE.1	завершено
FTP_TRP.1	завершено

FAU_GEN.1 – уточнен относительно ПЗ в связи с необходимостью генерировать записи аудита, связанные с ФТБ, не включенными в ПЗ.

FDP_ACF.1 – уточнен относительно ПЗ в связи с особенностями ОО – возможностью осуществлять политику дискреционного доступа к объектам, основываясь, в том числе и на привилегиях субъекта.

7.3 Дополнение ПЗ

В настоящее ЗБ включены политики безопасности, не вошедшие в ПЗ ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003»:

P.Warn – включена в связи с дополнительной возможностью ОО – предупреждением пользователей относительно несанкционированного использования ОО.

P.Sec – включена в связи с дополнительной возможностью ОО – обеспечением защиты аутентификационных данных, передаваемых доверенным удаленным системам ИТ.

P.FiltrationFlow – включена в связи с дополнительной возможностью ОО - осуществляться фильтрация входящих/исходящих в/из ОО информационных потоков.

В настоящее ЗБ включены следующие цели безопасности для ОО, не вошедшие в ПЗ ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003»:

O.Legal_Warning – ФБО должны располагать механизмами оповещения пользователя об ответственности за использования ОО до предоставления доступа к ресурсам, управляемым ФБО.

O.Sec – ФБО должны располагать механизмами, обеспечивающими защиту передаваемых данных ФБО удаленным доверенным системам ИТ.

O.FiltrationFlow – ФБО должны располагать механизмами, осуществляющими фильтрацию входящих/исходящих в/из ОО информационных потоков.

В настоящее ЗБ включены следующие функциональные требования безопасности ОО, не вошедшие в ПЗ ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003»:

- FDP_IFC.1 «Ограниченное управление информационными потоками»;
- FDP_IFF.1 «Простые атрибуты безопасности»;
- FRU_PRS.1 «Ограниченный приоритет обслуживания»;
- FRU_RSA.1 «Максимальные квоты»;
- FTA_SSL.2 «Блокирование, инициированное пользователем»;

- FTA_TAB.1 «Предупреждение по умолчанию перед предоставлением доступа к ОО»;
- FPT_RCV.1 «Ручное восстановление».

8. Обоснование

В данном разделе дано обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ЗБ. В разделе «Обоснование» также демонстрируется справедливость утверждений о СФБ и соответствии ПЗ.

8.1 Обоснование целей безопасности

8.1.1 Обоснование целей безопасности для ОО

В таблице 8.1 приведено отображение целей безопасности для ОО на угрозы и политику безопасности организации.

Таблица 8.1 – Отображение целей безопасности на угрозы и политику безопасности организации

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Rezidual_Information	O.Manage	O.FiltrationFlow	O. Sec	O.Enforcement	O.Audit_Protection	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.SafeRecovery	O.SOFAuth
T.Audit_Corrupt									X						
T.Config_Corrupt										X					
T.Objects_Not_Clean				X											
T.Spoof											X				
T.Sysacc	X														
T.Unanth_Access	X									X					
T.Unauth_Modification										X					
T.Undetected_Actions			X												
T.User_Corrupt		X								X					
T.FailureTOE														X	

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Rezidual_Information	O.Manage	O.FiltrationFlow	O. Sec	O.Enforcement	O.Audit_Protection	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.SafeRecovery	O.SOFAuth
P.Accountability			X		X			X							
P.Authorized_Users	X				X			X							
P.Need_To_Know		X		X	X			X							
P.Authorization													X		
P.FiltrationFlow						X									
P.Warn												X			
P.Sec							X								
P.AOFAuth															X

O.Authorization

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.Sysacc** и **T. T.Unanth_Access** и реализацией политики безопасности организации **P.Authorized_Users**, так как обеспечивает доступ к защищаемым активам только уполномоченным на это пользователям ОО и администраторам ОО.

O. Discretionary_Access

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T. User_Corrupt** и реализацией политики безопасности P.Need_No_Know, так как обеспечивает возможность уполномоченным пользователям ОО и администраторам ОО 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 организации **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.Rezidual_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 ресурсов и предотвращает использование остаточной информации при доступе к ресурсам нескольких пользователей.

O.Manage

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **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 доступа к системе.

O.Enforcement

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **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.Unanth_Access, T.Unauth_Modification, T.User_Corrupt,** так

как обеспечивает защиту ФБО от внешних воздействий и предотвращает несанкционированный доступ к данным и ресурсам 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 администраторов ОО и пользователей ОО.

O.FiltrationFlow

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.FiltrationFlow**, так как обеспечивает наличие механизмов, осуществляющих фильтрацию входящих/исходящих в/из ОО информационных потоков.

O.Legal_Warning

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.Warn**, так как обеспечивает пользователей об ответственности за неуполномоченное использование ОО.

O.Limit_Authorization

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

O.Sec

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Sec**, так как обеспечивает защиту передаваемых системных данных.

O.SafeRecovery

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.FailureTOE**, так как обеспечивает возможность безопасного восстановления ОО после сбоев и отказов программного обеспечения.

O.SOFAuth

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.SOFAuth**, так как предоставляет механизм, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

8.1.2 Обоснование целей безопасности для среды

В таблице 8.2 приведено отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности организации.

Таблица 8.2 – Отображение целей безопасности для среды на предположения безопасности

	OE.Install	OE.Phisical	OE.Creden	OE.TOEConfig
A.Connect		X		
A.Peer	X			
A.Coop			X	
A.Manage	X			
A.NO_Evil_Adm	X			
A.Locate		X		
A.Protect		X		
A.TOEConfig				X

OE.Install

Достижение этой цели безопасности необходимо в связи с реализацией предположения 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.

OE.Phisical

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

OE.TOEConfig

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.TOEConfig,** так как обеспечивает установку конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

OE.Creden

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

8.2 Обоснование требований безопасности

8.2.1 Обоснование требований безопасности для ОО

8.2.1.1 Обоснование функциональных требований безопасности ОО

В таблице 8.3 представлено отображение функциональных требований безопасности ОО на цели безопасности для ОО.

Таблица 8.3 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Rezidual_Information	O.Manage	O.FiltrationFlow	O. Sec	O.Enforcement	O.Audit_Protection	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.SafeRecovery	O.SOFAuth
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_IFC.1						X									
FDP_IFF.1						X									
FDP_RIP.2				X											
FIA_AFL.1	X														X

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Rezidual_Information	O.Manage	O.FiltrationFlow	O. Sec	O.Enforcement	O.Audit_Protection	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.SafeRecovery	O.SOFAuth
FIA_ATD.1	X	X													
FIA_SOS.1	X														X
FIA_UAU.2	X														
FIA_UAU.7	X														
FIA_UID.2	X														
FIA_USB.1		X	X												
FMT_MOF.1	X				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										
FMT_MTD.1 (6)	X				X										
FMT_MTD.1 (7)	X				X										
FMT_MTD.1 (8)			X		X										
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										

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Rezidual_Information	O.Manage	O.FiltrationFlow	O. Sec	O.Enforcement	O.Audit_Protection	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.SafeRecovery	O.SOFAuth
FPT_RVM.1								X							
FPT_RCV.1														X	
FPT_SEP.1								X		X					
FPT_STM.1			X												
FPT_TST.1										X					
FRU_PRS.1	X														
FRU_RSA.1	X														
FTA_SSL.1	X														
FTA_SSL.2	X														
FTA_TAB.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 для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с целью **O.Auditing** и способствует ее достижению.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи

пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **O.Auditing** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченному администратору ОО всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает запрет всем пользователям доступ к чтению записей аудита, за исключением уполномоченных администраторов ОО, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **O.Auditing** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение поиска и сортировки данных аудита, основанных на определенных критериях (идентификатор пользователя, тип результата события (успех и/или отказ), источник события, категория события, код события, временной интервал совершения события, идентификатор учетной записи компьютера). 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 ОО по таким атрибутам, как идентификатор пользователя, тип результата события (успех и/или отказ), источник события, категория события, код события, временной интервал совершения события, идентификатор учетной записи компьютера. 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 хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. 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 ОО, если журнал аудита превысит определенный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целями **O.Auditing**, **O.Managed** и способствует их достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает предотвращение событий, подвергающихся аудиту, и останов ОО при переполнении журнала аудита. 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, именованных объектов 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, определении правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **O.Discretionary_Access** и способствует ее достижению.

FDP_IFC.1 Ограниченное управление информационными потоками

Выполнение требований данного компонента обеспечивает реализацию политики фильтрации информации для субъектов, информации и операций перемещения информации. Рассматриваемый компонент сопоставлен с целью **O.FiltrationFlow** и способствует ее достижению.

FDP_IFF.1 Простые атрибуты безопасности

Выполнение требований данного компонента обеспечивает осуществление политики фильтрации информации, основываясь на атрибутах безопасности, определении правил фильтрации. Рассматриваемый компонент сопоставлен с целью **O.FiltrationFlow** 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 ОО. При достижении определенного администратором ОО числа неуспешных попыток аутентификации некоторого лица, данное лицо лишается возможности предпринимать дальнейшие попытки пройти процедуру аутентификации. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.SOFAuth** и способствует их достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (пользователя ОО и администратора ОО) в качестве атрибутов безопасности идентификатора пользователя, принадлежность к группе, привилегии, права доступа к ОО. Рассматриваемый компонент сопоставлен с целями **O.Authorization**, **O.Discretionary_Access** и способствует их достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает предоставление механизма для верификации соответствия паролей определенным требованиям. Рассматриваемый компонент сопоставлен с целями **O.Authorization**, **O.SOFAuth** и способствует их достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа 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 вводимый пользователем пароль отображается 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 **с**убъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_USB.1 Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от имени этого субъекта доступа. 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 определенные действия над функциями из числа ФБО только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O. Manage** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для пользователя ОО, являющегося владельцем 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 предоставляет возможность удаления, очистки и создания журнала аудита только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O. Manage, O.Auditing** и способствует их достижению.

FMT_MTD.1 (2) Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации и просмотра контролируемых событий аудита только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O. Manage, O.Auditing** и способствует их достижению.

FMT_MTD.1 (3) Управление данными ФБО

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

FMT_MTD.1 (4) Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность инициализации аутентификационных данных только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O. Manage, O.Authorization** и способствует их достижению.

FMT_MTD.1 (5) Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации аутентификационных данных только уполномоченному администратору и пользователям ОО. Рассматриваемый компонент сопоставлен с целями **O. Manage, O.Authorization** и способствует их достижению.

FMT_MTD.1 (6) Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации продолжительности блокировки учетной записи пользователя после превышения порога неуспешных попыток аутентификации только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O. Manage, O.Authorization** и способствует их достижению.

FMT_MTD.1 (7) Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации минимально допустимой длины пароля только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O. Manage, O.Authorization** и способствует их достижению.

FMT_MTD.1 (8) Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации размера журнала аудита только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O. Manage, O.Authorization** и способствует их достижению.

FMT_MTD.2 Управление ограничениями данных ФБО

Выполнение требований данного компонента предоставляет возможность определения ограничений для порогового значения количества неуспешных попыток аутентификации только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО в пределах ОДФ, только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Limit_Authorization, O. Manage** и способствует их достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами в пределах ОДФ, только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Limit_Authorization, O. Manage** и способствует их достижению.

FMT_SAE.1 Ограниченная по времени авторизация

Выполнение требований данного компонента предоставляет возможность назначать срок действия для аутентификационных данных только уполномоченному администратору ОО. По истечении срока действия аутентификационных данных ФБО осуществляют блокирование ассоциированной с пользователем учетной записи. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_SMR.1 Роли безопасности

Данный компонент включен в ЗБ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО. Рассматриваемый компонент сопоставлен с целями **O.Limit_Authorization, O.Manage** и способствует их достижению.

FMT_SMR.1 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_RCV.1 Ручное восстановление

Выполнение требований данного компонента обеспечивает защиту данных ФБО при передаче удаленным доверенным системам ИТ (в т.ч. защиту аутентификационной информации при передаче на контролер домена). Рассматриваемый компонент сопоставлен с целью **O.Sec** 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 ЗБ, 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.

FPT_TST.1 Тестирование ФБО

Выполнение требований данного компонента обеспечивает целостность выполнения ФБО и предоставляет уполномоченному администратору ОО средства верификации целостности кода и данных ФБО. Рассматриваемый компонент сопоставлен с целью **O.Protect** и способствует ее достижению.

FRU_PRS.1 Ограниченный приоритет обслуживания

Выполнение требований данного компонента обеспечивает установление субъектам приоритетов и обеспечивает доступ к процессорному ресурсу на основе приоритетов. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FRU_RSA.1 Максимальные квоты

Выполнение требований данного компонента обеспечивает возможность реализации максимальных квот для томов файловой системы и объектов службы каталогов, которые отдельные пользователи могут использовать одновременно. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

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

FTA_SSL.2 Блокирование, инициированное пользователем

Выполнение требований данного компонента обеспечивает блокирование сеанса, инициированное пользователем ОО или администратором ОО. 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 способность отказа ОО в открытии сеанса доступа к ОО, основываясь на идентификаторе пользователя, имени компьютера, сроке действия аутентификационных данных, времени доступа. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FTA_TAB.1 Предупреждения по умолчанию перед представлением доступа к ОО

Выполнение требований данного компонента обеспечивает отображение предупреждающего сообщения относительно несанкционированного использования ОО перед открытием сеанса пользователя. Рассматриваемый компонент сопоставлен с целью **O.Legal_Warning** и способствует ее достижению.

FTP_TRP.1 Доверенный маршрут

Выполнение требований данного компонента обеспечивает установление доверенной связи между ФБО и локальным пользователем ОО или администратором ОО для целей начальной аутентификации и разблокирования сеанса. Рассматриваемый компонент сопоставлен с целью **O.TrustedPath** и способствует ее достижению.

8.2.1.2 Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ЗБ соответствуют ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), и сформулированы, исходя из соответствия настоящего ЗБ профилю защиты ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003».

Выбор ОУД1 в качестве основы требований доверия в настоящем ЗБ является достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.

8.2.2 Обоснование зависимостей требований

В таблице 8.4 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены в настоящем ЗБ либо включением компонентов, определенных в части 2 ОК под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 ОК под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 8.4 является справочным и содержит компоненты, определенные в части 2 ОК в описании компонентов требований, приведенных в столбце 1 таблицы 8.4, под рубрикой «Зависимости».

Столбец 3 таблицы 8.4 показывает, какие компоненты требований были реально включены в настоящий ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 8.4. Компоненты требований в столбце 3 таблицы 8.4 либо совпадают с компонентами в столбце 2 таблицы 8.4, либо иерархичны по отношению к ним.

Таблица 8.4 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2
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

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
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_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2
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_SMR.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 , FMT_SMR.1
FMT_MTD.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (3)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (4)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (5)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (6)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (7)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (8)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	FMT_MTD.1 , FMT_SMR.1
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_SAE.1	FMT_SMR.1,	FMT_SMR.1,

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
	FPT_STM.1	FPT_STM.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RCV.1	FPT_TST.1, AGD_ADM.1, ADV_SPM.1	FPT_TST.1, AGD_ADM.1, *обосновано невключение ADV_SPM.1*
FPT_TST.1	FPT_AMT.1	FPT_AMT.1
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2
FTA_SSL.2	FIA_UAU.1	FIA_UAU.2

Включение в ЗБ компонента FPT_RCV.1 требует для удовлетворения зависимостей включения компонента ADV_SPM.1, однако разработчиком в руководствах ОО предоставлено четкое определение безопасного состояния ФБО, при котором ФБО не противоречивы и продолжают корректное осуществление ПБО, и объяснение, почему такое состояние можно считать безопасным; в связи с этим зависимость компонента FPT_RCV.1 от компонента ADV_SPM.1 не учитывается.

Все остальные зависимости включенных в ЗБ функциональных компонентов удовлетворены.

8.3 Обоснование краткой спецификации ОО

Обоснование краткой спецификации ОО представлено таблицей 8.5 и таблицей 8.6.

Таблица 8.5 – Отображение функциональных требований безопасности на функции безопасности

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Использование ресурсов ОО	Блокирование сеанса
FAU_GEN.1	X						
FAU_GEN.2	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_IFC.1		X					
FDP_IFF.1		X					
FDP_RIP.1		X					
FIA_AFL.1			X				
FIA_ATD.1			X				

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Использование ресурсов ОО	Блокирование сеанса
FIA_SOS.1			X				
FIA_UAU.2			X				
FIA_UAU.7			X				
FIA_UID.2			X				
FIA_USB.1			X				
FMT_MOF.1				X			
FMT_MSA.1				X			
FMT_MSA.3				X			
FMT_MTD.1 (1)	X			X			
FMT_MTD.1 (2)				X			
FMT_MTD.1 (3)				X			
FMT_MTD.1 (4)				X			
FMT_MTD.1 (5)				X			
FMT_MTD.1 (6)				X			
FMT_MTD.1 (7)				X			
FMT_MTD.1 (8)	X						
FMT_MTD.2				X			
FMT_REV.1 (1)		X		X			
FMT_REV.1 (2)							
FMT_SAE.1				X			

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Использование ресурсов ОО	Блокирование сеанса
FMT_SMR.1				X			
FMT_SMR.3					X		
FPT_RCV.1					X		
FPT_RVM.1					X		
FPT_SEP.1					X		
FPT_STM.1					X		
FPT_TST.1					X		
FRU_PRS.1						X	
FRU_RSA.1						X	
FTA_SSL.1							X
FTA_SSL.2							X
FTA_TSE.1							
FTP_TRP.1			X				
FTA_TAB.1			X				

Таблица 8.6 – Отображение требований доверия на меры безопасности

	Управление конфигурацией	Предоставление руководств	Предоставление проектной документации	Тестирование	Оценка стойкости функций безопасности
ACM_CAP.1	X				
ADO_IGS.1		X			
ADV_FSP.1			X		
ADV_RCR.1			X		
AGD_ADM.1		X			
AGD_USR.1		X			
ATE_IND.1				X	
AVA_SOF.1					X

8.4 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 ЗБ 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 СФБ в ЗБ определялся, исходя из возможностей ОО и обеспечения соответствия ОО профилю защиты ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003». Выбор средней СФБ в качестве минимального уровня

стойкости функций безопасности является достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.

8.5 Обоснование утверждений о соответствии ПЗ

Объект оценки соответствует профилю защиты ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

8.5.1 Обоснование конкретизации требований безопасности ИТ

Все требования безопасности, сформулированные в ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Операции подобных требований завершены в настоящем ЗБ в полном объеме.

Исходя из особенностей рассматриваемого ОО, по отношению к ряду функциональных требований, взятых из ПЗ, в настоящем ЗБ была применена операция уточнения.

FAU_GEN.1 – уточнено относительно ПЗ в связи с необходимостью генерировать записи аудита, связанные с функциональными возможностями ОО, не включенными в ПЗ.

FDP_ACF.1 – уточнено относительно ПЗ в связи с особенностями ОО – наличием у пользователей ОО такого атрибута безопасности, как привилегии.

8.5.2 Обоснование добавления политик безопасности организации

В настоящее ЗБ включены следующие политики безопасности организации, не вошедшие в ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003»:

P.Warn – включена в связи с возможностью ОО предупреждать пользователей относительно несанкционированного использования ОО.

P.Sec – включена в связи с возможностью ОО обеспечивать защиту аутентификационных данных, передаваемых доверенным удаленным системам ИТ.

P.FiltrationFlow – включена в связи с возможностью ОО осуществлять фильтрацию входящих/исходящих в/из ОО информационных потоков.

8.5.3 Обоснование добавления целей безопасности для ОО

В настоящее ЗБ включена следующие цели безопасности для ОО, не вошедшие в ПЗ ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003»:

O.Legal_Warning – ОО должен располагать механизмами оповещения пользователя об ответственности за использования ОО до предоставления доступа к ресурсам, управляемым ФБО.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ политики безопасности организации **P.Warn** и необходимостью ее реализации,.

O.Sec – ОО должен располагать механизмами, обеспечивающими защиту передаваемых данных ФБО удаленным доверенным системам ИТ.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ политики безопасности **P.Sec** и необходимостью противостояния ей.

O.FiltrationFlow – ОО должен располагать механизмами, осуществляющими фильтрацию входящих/исходящих в/из ОО информационных потоков.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ политики безопасности организации **P.FiltrationFlow** и необходимостью ее реализации.

8.5.4 Обоснование добавления требований безопасности ИТ

В настоящее ЗБ включены следующие функциональные требования безопасности ОО, не вошедшие в ПЗ ОС.КОС.ПЗ «Безопасность информационных технологий. Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003»:

Компонент функциональных требований безопасности FDP_IFC.1 – включен в связи с возможностью ОО реализовывать политику фильтрации информации.

Компонент функциональных требований безопасности FDP_IFF.1 – включен в связи с возможностью ОО осуществлять фильтрацию входящих информационных

потоков по определенным правилам, с использованием определенных атрибутов и в соответствии с политикой фильтрацией информации.

Компонент функциональных требований безопасности FRU_PRS.1 – включен в связи с возможностью ОО установления приоритетов каждому процессу и обеспечения доступа к процессорному ресурсу на основе установленных приоритетов.

Компонент функциональных требований безопасности FRU_RSA.1 – включен в связи с возможностью ОО реализации максимальных квот томов файловой системы.

Компонент функциональных требований безопасности FTA_SSL.2 – включен в связи с возможностью ОО реализации блокирования сеанса, инициированное уполномоченным администратором или уполномоченным пользователем.

Компонент функциональных требований безопасности FTA_TAB.1 – включен в связи с возможностью ОО реализации предупреждающего сообщения пользователю о несанкционированном использовании ОО.

Компонент функциональных требований безопасности FPT_RCV.1 – включен в связи с возможностью ОО реализации ручного восстановления ОО при сбоях или других прерываниях.