Операционная система
Microsoft® Windows® XP Professional Service Pack 3

Задание по безопасности

MS.Win_XP_SP3.ЗБ

Версия 1.00

2008

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД – база данных

ЗБ – задание по безопасности

ИТ – информационные технологии

ОДФ – область действия ФБО

ОК – Общие критерии

ОО – объект оценки

ОУД – оценочный уровень доверия к безопасности

ПБО – политика безопасности ОО

ПЗ – профиль защиты

ПФБ – политика функции безопасности

СФБ – стойкость функции безопасности

ФБО – функции безопасности ОО

ФТБ – функциональные требования безопасности

1 Введение ЗБ

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

1.1 Идентификация ЗБ

Название ЗБ:	Операционная система Microsoft® Windows® XP Professional Service Pack 3. Задание по безопасности.
Версия ЗБ:	Версия 1.00.
Обозначение:	MS.Win_XP_SP3.ЗБ.
Идентификация ОО:	Операционная система Microsoft® Windows® XP Professional Service Pack 3.
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. Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999. ISO/IEC 15408:1999.
Ключевые слова:	Операционная система, средство защиты информации, дискреционное управление доступом, задание по безопасности, ОУД1, Microsoft® Windows®.

1.2 Аннотация ЗБ

Настоящий ЗБ определяет требования безопасности для операционной системы Microsoft® Windows® XP Professional Service Pack 3 (далее – объект оценки).

Объект оценки (ОО) – клиентская многозадачная и многопользовательская операционная система, обеспечивающая управляемый доступ субъектов к объектам доступа. ОО располагает возможностями по управлению используемыми аппаратными средствами.

1.3 Соответствие ОК

Объект оценки и ЗБ согласованы со следующими спецификациями:

- профиль защиты «Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003» (соответствие ПЗ).
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002 (соответствие 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, ОУД1+).

1.4 Соглашения

Общие критерии допускают 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 **полужирным текстом**.

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 «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

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

1.5 Термины и определения

В настоящем ЗБ применяются следующие термины с соответствующими определениями.

Активы – информация или ресурсы, подлежащие защите контрмерами ОО.

Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора.

Аутентификация – процесс установления подлинности информации, предъявленной пользователем или объектом при регистрации.

Достоверность – свойство, 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.

Идентификатор – уникальный признак уполномоченного субъекта, однозначно его идентифицирующий.

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

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

Объект оценки – подлежащие оценке продукт ИТ или система ИТ с руководствами администратора или пользователя.

Подконтрольность – свойство, обеспечивающее однозначное отслеживание действий объектов и субъектов информационных отношений.

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

Политика функции безопасности – политика безопасности, осуществляемая ФБ.

Пользователь – любая сущность (человек-пользователь или внешняя сущность ИТ) вне ОО, которая взаимодействует с ОО.

Администратор ОО – группа уполномоченных пользователей, ответственных за установку, администрирование и эксплуатацию ОО.

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.

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 (носители информации, периферийные устройства, вычислительные возможности).

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

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

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

Функция безопасности – функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

Целостность – свойство поддержания 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 среды функционирования и границ ОО, служащее цели лучшего понимания его требований безопасности и дающее представление о типе продукта.

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

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

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

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

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

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 Microsoft® Windows® XP Professional Service Pack 3.

2.1 Тип продукта ИТ

Microsoft® Windows® XP Professional Service Pack 3 – клиентская многозадачная и многопользовательская операционная система со встроенной поддержкой одноранговых и клиент-серверных сетей и стека протоколов TCP/IP и IPX/SPX. Она позволяет обеспечить взаимодействие с сетями Novell, UNIX и AppleTalk. В состав Microsoft® Windows® XP Professional Service Pack 3 включен сервер IIS (Internet Information Sever v.6.0), предоставляющий платформу для размещения веб-узлов в сетях интранет.

Платформа Microsoft® Windows® XP Professional Service Pack 3 предоставляет широкие возможности по управлению используемыми аппаратными и вычислительными ресурсами, такими как процессорное время, память, устройства ввода-вывода и т.д.

Microsoft® Windows® XP Professional Service Pack 3 обеспечивает интуитивно понятный пользовательский интерфейс, расширенное управление электропитанием и поддержку технологии UPnP (Universal Plug and Play), позволяющей устранить ручное конфигурирование и обеспечить автоматическое обнаружение разных устройств.

Объект оценки характеризуется как управляемая, надежная и безопасная система, что достигается за счет использования файловой системы NTFS, средств управления приложениями и расширенных возможностей обеспечения безопасности, таких как встроенный брандмауэр, управляемый доступ к сети, технологии определения безопасности подключаемых в сеть систем (NAP), единый вход в систему, безопасное хранение реквизитов пользователя и т.д.

2.2 Основные функциональные возможности Microsoft® Windows® XP Professional Service Pack 3

В Microsoft® Windows® XP Professional Service Pack 3 имеется ряд возможностей и средств, упрощающих администрирование и управление средой, позволяющих обеспечить безопасность и надежность. В данном разделе представлена краткая спецификация данных функциональных возможностей.

2.2.1 Основные функциональные возможности обеспечения безопасности

В Microsoft® Windows® XP Professional Service Pack 3 включены средства, позволяющие защитить выбранные файлы, приложения и прочие ресурсы. В число этих средств входят списки управления доступом (ACL — Access Control Lists), группы безопасности и групповая политика, 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

В Microsoft® Windows® XP Professional Service Pack 3 имеется широкий набор шаблонов политик, которые могут применяться для управления как конфигурацией пользователей, так и настройками компьютера в конкретной вычислительной среде. Применение групповой политики осуществляется с целью контроля использования программ, сетевых ресурсов и операционной системы пользователями и компьютерами.

Групповые политики позволяют легко и единообразно управлять настройками большого количества вариантов среды настольных компьютерных систем путем выборочного включения и выключения отдельных функций.

Интегрирование групповой политики со службой каталогов Active Directory позволяет обеспечить большую безопасность и гибкость управления пользователями и объектами сети, позволяя администраторам объединить их в логические группы, такие как организационные подразделения, а затем назначать группам единые параметры конфигурации, что обеспечит непротиворечивость конфигураций разных членов групп. Задание соответствующих параметров групповой политики для определенных пользователей в сочетании с разрешениями NTFS, механизмом обязательных профилей и другими средствами безопасности Microsoft® Windows® XP Professional Service Pack 3, позволяет обеспечить безопасную среду для пользователя, ограничив их доступ к запрещенным программам и данным, системным параметрам Microsoft® Windows® XP Professional Service Pack 3, исключить вероятность модификации файлов системной конфигурации. Средства групповой политики позволяют обеспечить пользователей полностью настроенным рабочим столом, осуществить автоматическую установку

приложений, автоматизацию выполнения заданий или программ в момент входа или выхода пользователя или в момент включения или выключения компьютера.

Выделяют следующие основные функции групповой политики, поддерживаемые Microsoft® Windows® XP Professional Service Pack 3:

– **пользовательские политики**

Применяются к отдельным пользователям. ОО поддерживает возможность назначать выполнение сценариев, перенаправляет папки, управляет настройкой приложений, хранит предпочтения и настройки пользователя. Эти настройки политики действуют для данного пользователя на любом компьютере с установленным Microsoft® Windows® XP Professional Service Pack 3.

– **политики для компьютеров**

Позволяют управлять средствами безопасности, контролем доступа и настройками компьютера. Поддерживаются политики учетных записей, открытых ключей, сценарии, выполняемые при включении и выключении компьютера, локальные политики (аудит, назначение прав пользователей и параметров безопасности), а также политики IP-безопасности.

– **локальная политика безопасности**

Применяется для непосредственного изменения политик учетных записей и локальных политик, политик открытых ключей и политик IP-безопасности. Локальные политики предоставляются для учетных записей пользователей, не входящих в домен и для локальных политик компьютеров. Однако в большинстве случаев политика домена имеет приоритет по отношению к локальной политике безопасности.

2.2.1.2 Политики ограниченного использования программ

С помощью политик ограниченного использования программ в Microsoft® Windows® XP Professional Service Pack 3 реализуется ясный и понятный способ изоляции подозрительного, потенциально опасного кода, благодаря которому обеспечивается защита компьютера от различных вирусов, «троянских коней» и «червей», распространяемых через электронную почту. Эти политики предоставляют пользователю возможность выбрать способ, с помощью которого он будет осуществлять управление

программными продуктами на своем компьютере. Программный продукт может управляться «жестко» (пользователь сам решает, каким образом, когда и где будет происходить выполнение кода) или вообще не управляться (выполнение конкретного кода запрещено).

2.2.1.3 Группы безопасности

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

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

После установки в Microsoft® Windows® XP Professional Service Pack 3 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 (built-in local group);
- встроенные доменные локальные группы (built-in domain local group);
- встроенные глобальные группы (built-in global group).

2.2.1.4 Списки управления доступом

В Microsoft® Windows® XP Professional Service Pack 3 доступ к ресурсам системы разрешен только уполномоченным на это пользователям. Модель защиты Microsoft® Windows® XP Professional Service Pack 3 включает компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа, и аудит событий.

Каждый объект доступа, представленный в Microsoft® Windows® XP Professional Service Pack 3, однозначно ассоциирован с дескриптором безопасности, главными компонентами которого являются: дискреционный список контроля доступа, который собственно и определяет права доступа к объекту и системный список контроля доступа, служащий для назначения аудита. Список управления доступом включает перечень

пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

2.2.1.5 Аудит событий безопасности

В Microsoft® Windows® XP Professional Service Pack 3 имеется достаточный набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, и событий, которые могут произойти в вычислительной среде. 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 пользователей и учетными записями групп, 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 событий должен проводиться аудит.

2.2.1.6 Защита файлов

Подсистема WFP (Windows File Protection) обеспечивает защиту от перезаписи и удаления защищаемых системных файлов (*.sys, *.dll, *.ocs, *.ttf, *.exe и некоторые файлы *.fon). 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.

Системные файлы могут заменяться только сервисными пакетами Microsoft® Windows® XP Professional Service Pack 3, распространяемыми модулями обновлений, а также службой автоматического обновления Windows. 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, Microsoft® Windows® XP Professional Service Pack 3 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.

2.2.1.7 Криптографический модуль ядра

Новый криптографический модуль ядра rsaenh.dll содержащийся в Microsoft® Windows® XP Professional Service Pack 3, включает алгоритмы хэширования SHA2 (SHA256, SHA384, SHA512 сертификат X.509), что обеспечивает максимальную защиту шифрования данных системы.

2.2.1.8 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» вход на компьютер из сети может быть осуществлен только с учетной записью гостя. В классической модели безопасности пользователи, пытающиеся войти из сети на локальный компьютер, идентифицируются под своими учетными записями. Для компьютеров, входящих в домен, эта политика не применяется. Для всех других компьютеров по умолчанию используется политика принудительного применения учетной записи гостя.

Если действует 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 ресурсам данного компьютера. Если эта политика включена, всем локальным пользователям, пытающимся непосредственно подключиться к

компьютеру, предоставляется уровень разрешений гостя, который, как правило, существенно ограничен.

2.2.1.9 Ограничения на пустой пароль

Чтобы защитить пользователей, которые не применяют пароль в своих учетных записях, в Microsoft® Windows® XP Professional Service Pack 3 учетные записи, не имеющие пароля, применяются только для входа с физической консоли компьютера. Запрещается применять по умолчанию учетные записи с пустым паролем для удаленного входа на компьютер через сеть или для других действий, предусматривающих вход на компьютер. Исключением является вход с основной физической консоли. В частности, нельзя применять в качестве локального пользователя с пустым паролем службу вторичного входа в систему (службу RunAs) для запуска программ.

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

2.2.1.10 Управление учетными данными

Функция управления учетными данными обеспечивает безопасное хранение учетных данных пользователя, включая пароли и сертификаты X.509. Пользователям, включая перемещающихся пользователей, 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, их не потребуется вводить повторно.

2.2.1.11 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). Целевая информация, возвращаемая ресурсом, влияет на хранение учетных данных.

2.2.2 Основные функциональные возможности обеспечения функционирования

2.2.2.1 Мониторинг завершения работы

Microsoft® Windows® XP Professional Service Pack 3 содержит утилиту мониторинга завершения работы (Shutdown Event Tracker), обеспечивающую 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.

2.2.2.2 Архивация данных

В Microsoft® Windows® XP Professional Service Pack 3 входят стандартные средства предотвращения потери данных и их восстановления. Имеющаяся программа архивации и системные средства предоставляют пользователям возможность выполнять архивирование файлов и папок на несъемные и съемные устройства хранения. 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.

2.2.2.3 Теневое копирование тома

Управляет созданием теневых копий (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления или для иных целей.

2.2.2.4 Откат драйверов

Данная возможность способствует обеспечению устойчивости системы. 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 Driver (Драйвер) для соответствующего устройства и нажав кнопку Roll Back Driver (Откатить). Откат драйвера разрешается производить для одного уровня отката, поскольку только одна версия предыдущего драйвера может сохраняться при выполнении обновления. Данная возможность доступна для всех классов устройств, за исключением принтеров.

2.2.2.5 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 Microsoft® Windows® XP Professional Service Pack 3 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.

2.2.2.6 Аварийное восстановление системы

Функция аварийного восстановления системы (ASR – Automated System Recovery) позволяет сохранять и восстанавливать приложения. Эта функция обеспечивает реализацию механизма технологии Plug and Play, который используется для архивации соответствующих разделов реестра и восстановления данной информации в реестре. 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 функция ASR может быть использована для восстановления архивированных серверных данных.

2.2.3 Основные функциональные возможности администрирования, управления и поддержки

Средства администрирования, управления и поддержки обеспечивают полномасштабное и гибкое управление Microsoft® Windows® XP Professional Service Pack 3. Краткое описание основных из них представлено ниже.

2.2.3.1 Использование дисковых квот

Механизм дисковых квот позволяют отслеживать и контролировать использование пользователями места на диске для томов NTFS. Администраторы могут настроить Microsoft® Windows® XP Professional Service Pack 3 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 применяются только к томам и не зависят ни от структуры папок на томах, ни от схемы размещения томов на физических дисках. Квоты можно включать на локальных томах, сетевых томах и съемных дисках с файловой системой NTFS.

2.2.3.2 Инструментарий управления

Инструментарий управления Windows (Windows Management Instrumentation) представляет собой реализацию корпорации 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 (Microsoft Management Consol)

Консоль управления Microsoft Management Console 3.0 (MMC) – средство для создания, сохранения и открытия средств администрирования (называемых консолями MMC), которые управляют оборудованием, программными и сетевыми компонентами Microsoft® Windows® XP Professional Service Pack 3.

MMC не выполняет административные функции, но на ней размещаются инструменты, выполняющие эти функции. Основным типом инструментов, которые можно добавить на консоль, является оснастка. Другими добавляемыми элементами являются элементы управления ActiveX, ссылки на веб-страницы, папки, виды панели задач и задачи. Все функции управления в Microsoft® Windows® XP Professional Service Pack 3 доступны через оснастки консоли управления MMC.

2.2.3.4 Средства администрирования

В составе Microsoft® Windows® XP Professional Service Pack 3 интегрированы следующие средства администрирования:

- **службы компонентов** – используются администраторами администрирования программ COM+ из графического интерфейса, а также для автоматизации административных задач с помощью языков программирования и подготовки сценариев. Разработчики программного обеспечения могут использовать службы компонентов для наглядной настройки стандартных действий компонентов и программ, например, безопасности и участия в операциях, а также для интеграции компонентов в программы COM+;
- **управление компьютером** – используется для управления локальными или удаленными компьютерами одной, объединенной служебной программой рабочего стола. Оснастка «Управление компьютером» объединяет несколько средств администрирования Microsoft® Windows® XP Professional Service Pack 3 в одно дерево консоли, что обеспечивает легкий доступ к свойствам администрирования конкретного компьютера;
- **источники данных (ODBC)** – ODBC (Open Database Connectivity) – это 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 собираются сведения о неисправностях оборудования и неполадках программного обеспечения, а также отображаются события безопасности;
- **локальная политика безопасности** – используется для настройки параметров безопасности локального компьютера. Такими параметрами, помимо прочих, являются политика паролей, политика учетных записей, политика аудита, политика безопасности IP, определение присвоения прав пользователям, назначения агентов восстановления зашифрованных данных. 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;

- **системный монитор** – используется для сбора и просмотра в реальном времени данных о памяти, диске, процессоре, сети и других процессах в виде графика, гистограммы или отчета;
- **службы** – используется для управления службами компьютера, установки действий по восстановлению в случае сбоя службы и создания пользовательских имен и описаний служб для упрощения их определения;
- **центр обеспечения безопасности** – используется для управления настройками и работой брандмауэра Windows.

2.2.3.5 Результирующий набор политик

Средство «Результирующий набор политик» (RSoP – Resultant Set of Policy) в Microsoft® Windows® XP Professional Service Pack 3 позволяет администраторам просматривать результат применения групповой политики для указанного пользователя или компьютера. RSoP выступает в роли мощного и гибкого средства базового уровня для планирования, мониторинга и устранения неполадок при работе с групповой политикой.

2.2.3.6 Перемещение файлов конфигурации

Мастер перемещения файлов и конфигурации служит для переноса рабочих и конфигурационных файлов пользователя с одной рабочей станции на другую путем выполнения пошаговых инструкций. Мастер позволяет выбрать предназначенные для переноса файлы, их типы и папки. Поддерживается также перенос настроек для ограниченного набора приложений, включая приложения Microsoft Office.

2.2.3.7 Быстрое переключение пользователей одного компьютера

Функция быстрого переключения пользователей (Fast User Switching) позволяет нескольким лицам работать с компьютером так, как если бы он принадлежал каждому из них. Нет необходимости обеспечивать выход из системы другого пользователя или принимать решение, сохранять ли его файлы. Вместо этого в Microsoft® Windows® XP Professional Service Pack 3 применяется технология службы терминалов (Terminal Services) для запуска уникальных сеансов пользователей, что позволяет полностью разделить данные различных пользователей. Если применяются пароли пользователей, эти сеансы являются взаимно безопасными.

2.2.4 Основные функциональные возможности обеспечения сетевой безопасности и обеспечения безопасности при межсетевом взаимодействии

2.2.4.1 Контролируемый доступ к сети

В Microsoft® Windows® XP Professional Service Pack 3 имеются встроенные средства безопасности, позволяющие не допустить несанкционированного вторжения. Это достигается путем ограничения привилегий тех субъектов, кто пытается получить удаленный доступ к компьютеру, уровнем «гость». Работа системы 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.

Microsoft® Windows® XP Professional Service Pack 3 по умолчанию устанавливает для всех пользователей, входящих удаленно, учетную запись гостя. Благодаря этому предотвращаются попытки злоумышленников получить удаленный доступ к компьютеру посредством локальной учетной записи администратора, не имеющей пароля.

2.2.4.2 Брандмауэр Windows (Windows Firewall)

Microsoft® Windows® XP Professional Service Pack 3 обеспечивает защиту доступа в сети средствами встроенного брандмауэра Windows (Windows Firewall). Брандмауэр Windows обеспечивает защиту персонального компьютера с установленным Microsoft® Windows® XP Professional Service Pack 3, непосредственно подключенного к сети, или персональных компьютеров и устройств, подключенных к компьютеру, через который осуществляется общий доступ к подключению к сетям общего доступа и на котором исполняется брандмауэр Windows.

Брандмауэр Windows использует механизм активной фильтрации пакетов. Это означает, что порты брандмауэра открываются динамически, только на время, необходимое для получения доступа к запрашиваемым услугам. Данная технология противодействует попыткам сканирования портов и ресурсов компьютера, в том числе папок и принтеров с общим доступом. При этом существенно снижается угроза внешних атак.

Брандмауэр Windows поддерживает подключения по коммутируемым каналам, локальной сети, виртуальным частным сетям и по протоколу Point-to-Point over Ethernet.

При включении брандмауэр Windows блокирует все несанкционированные подключения, поступающие через интерфейс публичной сети. Для этой цели в брандмауэре Windows применена NAT-таблица потоков (Network Address Translation - преобразование сетевых адресов) с проверкой любого входящего потока на соответствие записям в этой таблице. Входящие потоки данных пропускаются только в том случае, если в NAT-таблице потоков имеется соответствующее указание, исходящее из системы брандмауэра или из внутренней части защищенной сети. Иными словами, если обмен информацией не санкционирован из защищенной сети, входящие данные игнорируются.

2.2.4.3 Технология определения безопасности подключаемых в сеть систем (NAP)

Network Access Protection (NAP) позволяет безопасно функционировать с Windows Server 2008. NAP позволяет более эффективно защищать локальные сети путем определения безопасности подключаемых систем, например, наличие антивируса или установленных патчей. Если на момент соединения компьютер, подключаемый к сети, отвечает всем необходимым условиям безопасности, то доступ ему разрешается. Иначе машина помещается в карантинный сегмент сети который разрешает только ограниченный доступ к ресурсам.

2.2.4.4 Конфиденциальность персональных данных

Браузер Microsoft Internet Explorer 6.0 позволяет следить за персональными данными пользователя во время посещения веб-сайтов благодаря поддержке стандарта P3P (Platform for Privacy Preferences).

Данный стандарт позволяет пользователю принимать информированное решение относительно вида и объема информации, к которой он предоставляет доступ по сети. Браузер Internet Explorer 6.0 определяет, соответствует ли веб-сайт, который собирается посетить пользователь, стандартам консорциума W3C и сообщает ему статус веб-сайта, прежде чем отправлять конфиденциальную информацию.

После того как в Internet Explorer 6.0 определены параметры конфиденциальности, задающие уровень раскрытия информации, браузер определяет, совместим ли выбранный веб-сайт со стандартом P3P. Если условие совместимости выполняется, браузер

сравнивает заданные параметры конфиденциальности с соответствующей политикой, принятой на данном веб-сайте. Браузер Internet Explorer осуществляет обмен информацией о политике обеспечения конфиденциальности с помощью протокола HTTP. На основе заданных вами параметров конфиденциальности определяется, следует ли передавать персональные данные на данный веб-сайт.

2.2.4.5 Поддержка стандартов безопасности

Microsoft® Windows® XP Professional Service Pack 3 обеспечивает возможность поддержки безопасных сетей, построенных на основе последних стандартов безопасности, включая SSL/TLS, IPSec и Kerberos v.5.

IP-безопасность (IPSec)

Позволяет защитить данные, передаваемые по сети. IP-безопасность играет важную роль в обеспечении безопасности виртуальных частных сетей (VPN), обеспечивающих возможность безопасной передачи данных через сети общего пользования.

Поддержка протокола Kerberos

В Microsoft® Windows® XP Professional Service Pack 3 учетные данные могут быть представлены в виде пароля, мандата Kerberos или смарт-карты, если компьютер оборудован для работы со смарт-картами.

Протокол Kerberos V5 обеспечивает средства взаимной проверки подлинности клиентов, например пользователя, компьютера или службы и сервера. Благодаря поддержки протокола Kerberos V5 Microsoft® Windows® XP Professional Service Pack 3 предоставляет пользователям возможность однократного ввода аутентификационных данных для доступа ко всем ресурсам и поддерживаемым приложениям, права на доступ к которым у них имеются.

2.2.4.6 Единый вход с цифровым паспортом Microsoft

В Microsoft® Windows® XP Professional Service Pack 3 протоколы проверки подлинности цифрового паспорта были добавлены к WinInet, библиотеке DLL, с помощью которой компьютер может извлекать данные из различных источников, что

позволяет Microsoft® Windows® XP Professional Service Pack 3 очевидным образом использовать проверку подлинности цифрового паспорта. Если пользователь имеет цифровой паспорт Microsoft, он может автоматически использовать его для выполнения многих задач, таких как вход на веб-сайт, поддерживающий цифровые паспорта.

2.2.4.7 Поддержка безопасных беспроводных сетей Wi-Fi Protected Access 2 (WPA2)

В Microsoft® Windows® XP Professional Service Pack 3 реализована поддержка WPA2 или стандарта IEEE 802.11i, что намного увеличивает безопасность беспроводных каналов передачи данных.

2.2.4.8 Поддержка технологии Digital Identity Management Service (DIMS)

В Microsoft® Windows® XP Professional Service Pack 3, пользователи, залогинившиеся в любой компьютер домена, получат все свои сертификаты и приватные ключи приложений.

2.2.4.9 Технология определения "Black Hole" роутеров

В Microsoft® Windows® XP Professional Service Pack 3, администратор сможет идентифицировать роутеры, которые теряют пакеты и как следствие увеличить надежность передачи данных в сети.

2.2.5 Возможности масштабирования

Microsoft® Windows® XP Professional Service Pack 3 обеспечивает возможность масштабирования, что позволяет обеспечить поддержку больших томов и выполнение более сложных приложений.

Microsoft® Windows® XP Professional Service Pack 3 поддерживает до двух симметричных процессоров и до 4 гигабайтов оперативной памяти. Максимальный объем дискового пространства на одном томе не может превышать двух терабайт.

2.3 Среда функционирования и границы ОО

2.3.1 Среда функционирования

Среда функционирования определяется конфигурациями Enterprise, High Security и Stand-Alone.

Enterprise

Данная среда подразумевает наличие инфраструктуры домена Active Directory Windows Server 2003 или Windows 2000. Управление клиентами в данной среде происходит через использование групповой политики, применяемой на различных уровнях иерархии (сайты, домены, организационные подразделения). Групповые политики предоставляют механизм централизованного управления политиками безопасности для среды функционирования в целом.

High Security

Среда High Security подразумевает наличие более ограничивающей политики безопасности и усиленные настройки безопасности для клиентов. При применении данных настроек функциональность пользователя ограничивается полномочиями на выполнение только необходимых задач. Полномочия пользователя определяется политикой ограниченного использования программ и разрешенными службами.

Stand-Alone

Среда Stand-alone подразумевается такую организацию, которая предусматривает наличие компьютеров, которые не могут быть добавлены в домен, или компьютеров, являющихся членами домена Windows NT 4.0. Конфигурирование данных клиентов осуществляется через настройку параметров локальной политики.

2.3.2 Границы ОО

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

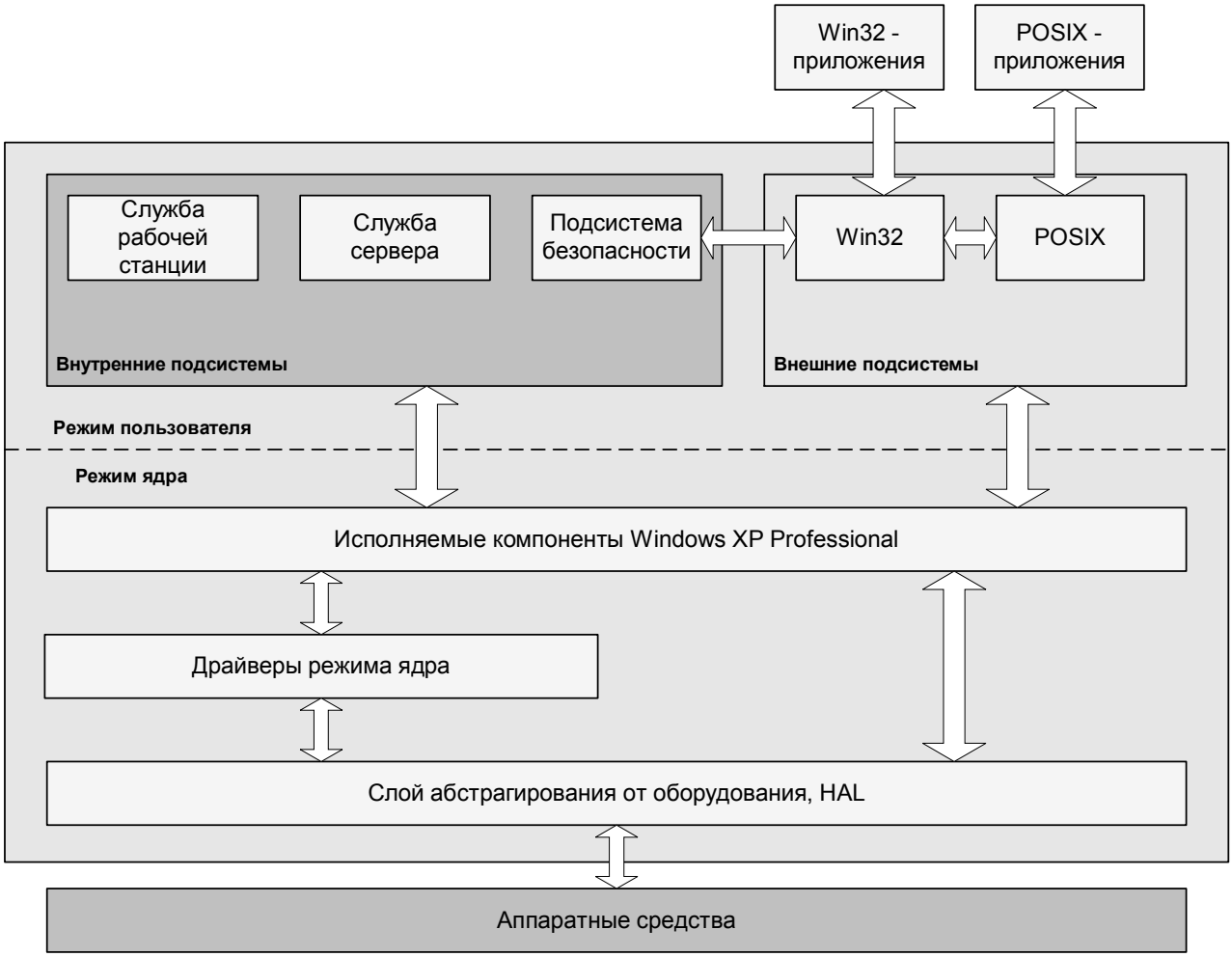

Рисунок 1 – Взаимодействие элементов объекта оценки

Уровень режима пользователя состоит из набора компонентов, называемых подсистемами, осуществляющих передачу запросов ввода-вывода драйверам режима ядра через службы ввода-вывода. Уровень режима пользователя позволяет управлять приложениями Win32 и обеспечивает работу приложений Win16 и MS-DOS.

Уровень режима ядра имеет доступ к системным данным и аппаратным средствам. Компоненты в режиме ядра могут напрямую обращаться к памяти и выполняются в защищенном адресном пространстве. Уровень режима ядра включает несколько типов компонентов, выполняющих строго определенные функции.

Объект оценки поддерживает вытесняющую многозадачность и способен работать, одинаково эффективно используя одно- и многопроцессорные системы. При этом гарантируется, что код, выполняемый на одном процессоре, не получит доступ и не

модифицирует данные, обрабатываемые другим процессором. ОО поддерживает пакетный ввод-вывод с применением возвратных пакетов запроса ввода-вывода и асинхронный ввод-вывод.

2.4 Службы безопасности ОО

Ниже представлено краткое описание служб безопасности ОО, реализующих оцениваемые (в соответствии с настоящим ЗБ) функции безопасности ОО.

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.

Защита данных пользователя

Объект оценки осуществляет функции и политику избирательного управления доступом, политику фильтрации 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, каталоги и принтера. Каждый пользователь, пытающийся получить доступ к системе, сначала проходит аутентификацию, 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 даны соответствующие права. Главными компонентами дескрипторами безопасности объекта являются: дискреционный список контроля доступа, который собственно и определяет права доступа к объекту и системный список контроля доступа, служащий для назначения аудита. ОО обеспечивает фильтрацию входящей в ОО информации (защиту доступа в сети) использованием брандмауэра Windows. 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.

Идентификация и аутентификация

Объект оценки требует, чтобы все субъекты доступа 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 базу данных (БД) безопасности, хранящую информацию об учетных записях пользователей. Каждая учетная запись представлена идентификатором пользователя, однозначно связанным с идентификатором безопасности – SID (Security Identificator, Security Identification Descriptor), 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 определённого количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором ОО или по истечению времени действия, заданного для счетчика блокировки.

Объект оценки позволяет администратору ОО задавать заголовок сообщений для пользователей при входе в систему.

Управление безопасностью

Объект оценки включает механизмы управления групповыми политиками. Групповая политика является важным средством обеспечения безопасности ОО и обеспечивает управление конфигурацией 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 контролируется посредством механизма управления доступом, членства в административных группах и назначаемых полномочий (привилегий).

Объект оценки включает компонент «Центр обеспечения безопасности», позволяющий осуществлять управление брандмауэром Windows.

Защита функций безопасности ОО

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

Использование ресурсов

Объект оценки может ограничивать объем доступного 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 и пределы квот, как для всех пользователей, так и индивидуально для каждого пользователя. Кроме того, администратор ОО полномочен определять действия, выполняемые при превышении квот пользователями.

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

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.

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 относительно предопределенного использования ОО

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.Trusted_Load

Загрузка ОО должна проходить в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование инструментальных средств, позволяющих осуществить доступ к защищаемым ресурсам ОО в обход механизмов защиты.

A.Disable_Debugger

Для предотвращения несанкционированного доступа к системным компонентам в ОО должна быть исключена возможность запуска встроенных программ отладки.

3.1.2 Предположения относительно среды функционирования ОО

Предположения, связанные с физической защитой ОО

A.Locate

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

A.Protect

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

Предположения, имеющее отношение к персоналу

A.Coop

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

A.Manage

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

A.No_Evil_Adm

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

3.2 Угрозы

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

T.Audit_Corrupt

1. Аннотация угрозы – модификация или удаление данных аудита неуполномоченными на это пользователями в нарушение политики безопасности.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – доступ к данным аудита и осуществление их модификации или удаления.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита.

5. Вид активов, потенциально подверженных угрозе – данные аудита.

6. Нарушаемое свойство безопасности активов – целостность.

7. Возможные последствия реализации угрозы – возможность совершения неконтролируемых действий.

T.Config_Corrupt

1. Аннотация угрозы – модификация конфигурационных данных неуполномоченными на это пользователями в нарушение политики безопасности.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – доступ к конфигурационным данным и осуществление их модификации.

4. Используемые уязвимости – недостатки механизмов защиты конфигурационных данных.

5. Вид активов, потенциально подверженных угрозе – конфигурационные данные.

6. Нарушаемое свойство безопасности активов – целостность.

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

T.Objects_Not_Clean

1. Аннотация угрозы – несанкционированный доступ пользователей к информации вследствие отсутствия надлежащих механизмов очистки информационного содержания освобождаемых совместно используемых объектов доступа.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – доступ к информации.

4. Используемые уязвимости – недостатки или отсутствие надлежащих механизмов очистки информационного содержания освобождаемых совместно используемых объектов доступа.

5. Вид активов, потенциально подверженных угрозе – информация.

6. Нарушаемое свойство безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – получение доступа к конфиденциальной информации неуполномоченными пользователями.

T.Spoof

1. Аннотация угрозы – хищение аутентификационных данных уполномоченных пользователей путем подмены сервисов доступа.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – подмена сервисов доступа.

4. Используемые уязвимости – недостатки механизмов защиты сервисов доступа от подмены.

5. Вид активов, потенциально подверженных угрозе – аутентификационные данные.

6. Нарушаемое свойство безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – осуществление доступа неуполномоченного пользователя, используя аутентификационные данные уполномоченного пользователя.

T.Sysacc

1. Аннотация угрозы – 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 режимов функционирования ОО или ограничения доступа к ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – несанкционированный доступ к ОО под видом администратора или другого уполномоченного пользователя.

4. Используемые уязвимости – недостатки механизмов разграничения доступа.

5. Вид активов, потенциально подверженных угрозе – ОО.

6. Нарушаемые свойства безопасности активов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, ограничение доступа к ОО.

T.Unauth_Access

1. Аннотация угрозы – доступ к системным данным со стороны неуполномоченных пользователей вследствие недостатков механизмов разграничения доступа.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – доступ к системным данным.

4. Используемые уязвимости – недостатки механизмов разграничения доступа.

5. Вид активов, потенциально подверженных угрозе – системные данные.

6. Нарушаемое свойство безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – проведение анализа системных данных с целью получения представления об уровне защищенности ОО.

T.Unauth_Modification

1. Аннотация угрозы – несанкционированный доступ к ОО и пользовательским данным путем модификации функций безопасности ОО вследствие недостатков механизмов защиты функций безопасности ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – модификация функций безопасности ОО.

4. Используемые уязвимости – недостатки механизмов защиты функций безопасности ОО.

5. Вид активов, потенциально подверженных угрозе – ОО и пользовательские данные.

6. Нарушаемое свойство безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – ознакомление с пользовательскими данными неуполномоченными пользователями.

T.Undetected_Actions

1. Аннотация угрозы – невыполнение регистрации несанкционированных действий вследствие недостатков механизмов аудита.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – несанкционированные действия.

4. Используемые уязвимости – недостатки механизмов аудита.

5. Вид активов, потенциально подверженных угрозе – ОО.

6. Нарушаемое свойство безопасности активов – конфиденциальность, целостность, доступность, подконтрольность.

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

T.User_Corrupt

1. Аннотация угрозы – модификация пользовательских данных неуполномоченными на это пользователями вследствие недостатков механизмов разграничения доступа к данным, осуществляемого уполномоченными пользователями.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – доступ к пользовательским данным.

4. Используемые уязвимости – недостатки механизмов разграничения доступа.

5. Вид активов, потенциально подверженных угрозе – пользовательские данные.

6. Нарушаемое свойство безопасности активов – целостность.

7. Возможные последствия реализации угрозы – потеря пользовательских данных.

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.Warn

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

P.Sec

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

P.Filtration

Объект оценки должен осуществлять фильтрацию входящих информационных потоков.

4 Цели безопасности

4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

O.Authorization

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

O.Discretionary_Access

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

O.Auditing

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

O.Residual_Information

ФБО должны обеспечивать недоступность информационного содержания освобождаемых защищаемых ресурсов.

O.Manage

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

O.Enforcement

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

O.Audit_Protection

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

O.Protect

В целях защиты от внешнего воздействия ФБО должны обеспечивать защиту собственных данных 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, управляемым ФБО.

O.Limit_Authorization

ФБО должны предоставлять возможность ограничивать уровень полномочий для каждого пользователя.

O.Sec

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

O.Filtration

ФБО должны располагать механизмами, осуществляющими фильтрацию входящих в ОО информационных потоков.

4.2 Цели безопасности для среды

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

OE.Install

Должна быть обеспечена поставка, установка, управление и функционирование ОО в соответствии с руководствами.

OE.Physical

Должна быть обеспечена защита критичных по безопасности частей ОО от физического воздействия, способного скомпрометировать цели безопасности.

OE.Creden

Должны быть обеспечены мероприятия по защите всей удостоверяющей информацией (пароли или другая аутентификационная информация).

OE.Trusted_Load

Должна быть обеспечена загрузка ОО в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование инструментальных средств, позволяющих осуществить доступ к защищаемым ресурсам ОО в обход механизмов защиты.

OE.Disable_Debugger

Для предотвращения несанкционированного доступа к системным компонентам в ОО должна быть исключена возможность запуска встроенных программ отладки.

5 Требования безопасности ИТ

В данном разделе ЗБ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, 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). В качестве минимального уровня стойкости функций безопасности, реализованных вероятностными или перестановочными механизмами, заявлена средняя СФБ.

5.1 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
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

Идентификатор компонента требований	Название компонента требований
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_AMT.1	Тестирование абстрактной машины
FPT_ITC.1	Конфиденциальность экспортируемых данных ФБО при передаче
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени
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

Идентификатор компонента требований	Название компонента требований
FTA_TAB.1	Предупреждения по умолчанию перед предоставлением доступа к ОО
FTA_TSE.1	Открытие сеанса с ОО
FTP_TRP.1	Доверенный маршрут

5.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

а) запуск и завершение выполнения функций аудита;

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

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

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

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

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_SAR.1	Чтение информации из записей аудита	
FAU_SAR.2	Неуспешные попытки читать информацию из записей аудита	
FAU_SEL.1	Все модификации конфигурации аудита,	

Компонент	Событие	Детализация
	происходящие во время сбора данных аудита	
FAU_STG.3	Предпринимаемые действия после превышения порога заполнения	
FAU_STG.4	Предпринимаемые действия при сбое хранения журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на объекте, на который распространяется ПФБ	Идентификатор объекта
FDP_IFF.1	Все решения по запросам на информационные потоки	
FIA_AFL.1	Блокирование учетной записи в результате превышения максимального числа неуспешных попыток входа в систему	
FIA_SOS.1	Отклонение или принятие ФБО любого проверенного пароля	
FIA_UAU.2	Все случаи использования механизма аутентификации	
FIA_UID.2	Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	
FIA_USB.1	Успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта)	
FMT_MOF.1 (1)	Все модификации политики аудита	
FMT_MSA.1 (1)	Все модификации значений атрибутов безопасности	
FMT_MSA.3 (1)	Модификации настройки по умолчанию	

Компонент	Событие	Детализация
	разрешающих или ограничительных правил. Все модификации начальных значений атрибутов безопасности	
FMT_MTD.1 (1)	Все модификации значений данных ФБО	
FMT_MTD.1 (2)	Все модификации значений данных ФБО	Новое значение данных ФБО
FMT_MTD.1 (3)	Все модификации значений данных ФБО	Новое значение данных ФБО
FMT_MTD.1 (4)	Все модификации значений данных ФБО	
FMT_MTD.1 (5)	Все модификации значений данных ФБО	
FMT_MTD.1 (8)	Попытка использовать привилегию уполномоченного администратора для изменения представления времени для ФБО	
FMT_MTD.2	Все модификации ограничений данных ФБО. Все модификации действий, предпринимаемых при нарушениях ограничений	
FMT_REV.1 (1)	Все попытки отменить атрибуты безопасности	
FMT_REV.1 (2)	Все попытки отменить атрибуты безопасности	
FMT_SAE.1	Назначение срока действия для атрибута. Действия, предпринятые по истечении назначенного срока	
FMT_SMR.1	Модификация группы пользователей – исполнителей роли. Каждое использование прав, предоставляемых ролью	Роль и начало запроса
FPT_AMT.1	Выполнение тестирования базовой	

Компонент	Событие	Детализация
	машины 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 [администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

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

Зависимости: FAU_GEN.1 «Генерация данных аудита».

FAU_SAR.2 Ограниченный просмотр аудита

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

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

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

[

следующих атрибутах:

а) идентификатор пользователя;

б) тип (успех и/или отказ), дата, время, категория, идентификатор события, 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 (успех и/или отказ), дата, время, категория, идентификатор события, идентификатор учетной записи компьютера].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 (2) «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 *предотвращать* 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 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***, и [других действий, которые нужно предпринять в случае возможного сбоя хранения журнала аудита, не предусмотрено] при переполнении журнала аудита.

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

5.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

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

[

а) 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), мьютекс (Mutant), 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) всех операций между субъектами и объектами

].

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

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

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

[

следующем:

а) ассоциированные с субъектом идентификатор пользователя, принадлежность к группе (группам) **и привилегии субъекта**;

б) следующие, ассоциированные с объектом, атрибуты 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 запрещаются 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) для следующих операций уполномоченный администратор может обойти правила, перечисленные в FDP_ACF.1.2:

– запрос на смену владельца объекта;

б) для следующих операций только уполномоченному администратору может быть предоставлен доступ и правила, определенные FDP_ACF.1.2, не применяются:

– запрос на смену или модификацию аудита попыток доступа к объекту

].

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

[

в доступе к объекту 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 (1) «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 в 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 ПФБ управления информационными потоками не заданы].

FDP_IFF.1.4 ФБО должны предоставить следующее [дополнительные возможности ПФБ 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 *распределении ресурсов* для всех объектов.

Зависимости: отсутствуют.

Замечание по применению:

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

5.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [определенное администратором ОО число] неуспешных попыток аутентификации, относящихся к [любому процессу входа пользователя в систему].

FIA_AFL.1.2 При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить [блокировку учетной записи пользователя продолжительностью, определенной уполномоченным администратором].

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 секреты отвечают

[

следующему:

а) для каждой попытки использования механизма аутентификации вероятность случайного доступа должна быть меньше, чем **$2{,}5x10^{-14}$**;

б) при неоднократных попытках использования механизма аутентификации в течение одной минуты вероятность случайного доступа должна быть меньше, чем **$2{,}5x10^{-14}$**;

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

].

Зависимости: отсутствуют.

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый **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].

FIA_USB.1.2 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].

FIA_USB.1.3 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».

5.1.4 Управление безопасностью (FMT)

FMT_MOF.1 (1) Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность *<u>определять режим выполнения, отключать, подключать, модифицировать режим выполнения</u>* функций**, связанных с:**

[

– аудитом;

– выполнением процедур очистки остаточной информации в файлах подкачки;
– назначением приоритетов каждому субъекту в ФБО;
– фильтрацией информации;
– квотированием томов NTFS для пользователей;
– определением условий, при которых происходит тестирование абстрактной машины и самотестирование;
– условиями открытия сеанса доступа,

]

оставив такую возможность только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MOF.1 (2) Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность *определять режим выполнения, отключать, подключать, модифицировать режим выполнения* функции**,** [блокирования сеанса пользователя] только [администратору ОО и пользователю ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (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 [администратору ОО; пользователю ОО, являющемуся владельцам объекта; пользователю ОО, имеющему право смены владельца; пользователю ОО, имеющему право модификации DACL].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (1) 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 создателем объекта] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта.

Зависимости: FMT_MSA.1 (1) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (2) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику фильтрации информации], **предоставляющую** возможность *модифицировать* ***атрибуты безопасности в правиле***, *удалять* ***атрибуты безопасности из правила***, [*добавлять атрибуты безопасности в правило*] **для атрибутов безопасности**, [перечисленных в элементе FDP_IFF.1.1 компонента FDP_IFF.1], только [администратору ОО].

Зависимости: FDP_IFC.1 «Ограниченное управление информационными потоками»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (3) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику фильтрации информации], **предоставляющую** возможность *удалять* [*создавать*] атрибуты безопасности **для** [правил управления информационными потоками, перечисленные в элементе FDP_IFF.1.2 компонента FDP_IFF.1], только [администратору ОО].

Зависимости: FDP_IFC.1 «Ограниченное управление информационными потоками»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (2) Инициализация статических атрибутов

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

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

Зависимости: FMT_MSA.1 (2) «Управление атрибутами безопасности»,
FMT_MSA.1 (3) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (1) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *удаления, очистки, [создания]* [журнала аудита] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (2) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации или [просмотра]* [множества подвергающихся аудиту событий] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (3) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации и [инициализации]* [атрибутов безопасности пользователя, кроме аутентификационных данных] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (4) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *[инициализации]* [аутентификационных данных] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (5) Управление данными ФБО

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

[

следующим:

а) администратору ОО;

б) пользователю ОО, имеющему право модифицировать собственные аутентификационные данные

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (6) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [продолжительности блокировки учетной записи пользователя после превышения порога неуспешных попыток аутентификации] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (7) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [минимально допустимой длины пароля] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (8) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [представления времени ФБО] только [администратору ОО].

Зависимости: FMT_SMR.1 Роли безопасности

FMT_MTD.1 (9) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [установок квотирования на томах NTFS] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (10) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [предупреждающего сообщения перед установлением сеанса пользователя] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (11) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [размера журнала аудита] только [администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 (12) Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *изменения значений по умолчанию, модификации, удаления, очистки* [порогового значения продолжительности бездействия уполномоченного пользователя в течение интерактивного сеанса] только [пользователю ОО, имеющему право модифицировать пороговое значение продолжительности бездействия при интерактивном сеансе].

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 [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 администратором ОО].

Зависимости: FMT_MTD.1 (3) «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 [администратору ОО].

FMT_REV.1.2 ФБО должны **осуществлять** правила

[

a) немедленной отмены имеющих отношение к безопасности полномочий;

б) [другие правила не предусмотрены]

].

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** правила

[

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

б) [другие правила отсутствуют]

].

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 [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) администратор ОО;

б) пользователь ОО;

г) [другие роли не определены]

].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** с ролями.

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

Замечание по применению:

В настоящем ЗБ при изложении функциональных требований безопасности роль «пользователь ОО» интерпретируется как:

- пользователь ОО, являющийся владельцем объекта;
- пользователь ОО, имеющий право смены владельца;
- пользователь ОО, имеющий право модификации DACL;
- пользователь ОО, являющийся создателем объекта;
- пользователь ОО, имеющий право модифицировать собственные аутентификационные данные;
- пользователь ОО, уполномоченный согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта;
- пользователь ОО, имеющий право модифицировать пороговое значение продолжительности бездействия при интерактивном сеансе.

FMT_SMR.3 Принятие ролей

FMT_SMR.3.1 ФБО должны требовать точный запрос для принятия роли [администратор ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

5.1.5 Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ *при первоначальном запуске, периодически во время нормального функционирования, по запросу уполномоченного пользователя* 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 защитить все данные ФБО, передаваемые от ФБО к 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_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».

5.1.6 Использование ресурсов (FRU)

FRU_PRS.1 Ограниченный приоритет обслуживания

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

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

Зависимости: отсутствуют.

FRU_RSA.1 Максимальные квоты

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

Зависимости: отсутствуют.

5.1.7 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 выбранного пользователя], для чего предпринимаются следующие действия:

а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;

б) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

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

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

FTA_SSL.2 Блокирование, инициированное пользователем

FTA_SSL.2.1 ФБО должны допускать инициированное пользователем 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].

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

FTA_TAB.1 Предупреждения по умолчанию перед предоставлением доступа к ОО

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

Зависимости: отсутствуют.

FTA_TSE.1 Открытие сеанса с ОО

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

Зависимости: отсутствуют.

5.1.8 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.

5.2 Требования доверия к безопасности ОО

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

Таблица 5.3 – Требования доверия к безопасности ОО

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

5.2.1 Управление конфигурацией (ACM)

ACM_CAP.1 Номера версий

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

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

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

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

5.2.2 Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

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

5.2.3 Разработка (ADV)

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_FSP.1.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

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

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

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

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

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

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

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

5.2.4 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

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

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

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

AGD_ADM.1.6C Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.

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

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

Элементы действий оценщика

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

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

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

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

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

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

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

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

Элементы действий оценщика

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

5.2.5 Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

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

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

5.2.6 Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

Элементы действий оценщика

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

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

6 Краткая спецификация ОО

6.1 Функции безопасности ОО

В данном разделе представлено описание функций безопасности ОО и их сопоставление с функциональными требованиями безопасности. ОО реализует следующие функции безопасности:

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

6.1.1 Функции безопасности ОО «Аудит безопасности»

Функции безопасности ОО «Аудит безопасности» обеспечивают:

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

6.1.1.1 Сбор данных аудита

За создание журнала безопасности, содержащего записи об относящихся к безопасности событиях, и регистрацию подвергаемых аудиту событий в ОО отвечает локальная служба «Регистратор событий» (Event Logger). Журнал безопасности содержит информацию о контролируемых политикой аудита событиях, таких как успешные и неуспешные попытки входа в ОО.

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

Можно проводить аудит как успешных, так и неуспешных попыток выполнения некоторых действий. При этом в журнал 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.
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, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала безопасности содержит оба кода. Имперсонация происходит в тех случаях, когда в ОО один процесс присваивает атрибуты безопасности другого процесса.
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 безопасности источник события определяется как «Security».
Тип	Уровень важности событий. В журналах аудита записи событий могут быть одного из пяти типов (см. таблицу 6.2). В окне просмотра событий тип события представлен соответствующим значком.
Категория	Категория события в зависимости от источника события. Для аудита событий безопасности категория соответствует одному из типов

Сведения	Описание
	событий, для которых в политике аудита может быть включен аудит успехов или отказов (см. таблицу 6.3).

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 журналы событий заносятся события пяти различных типов.

Таблица 6.2 – Типы событий

Тип события	Описание
Ошибка	Серьезные сложности, такие как потеря данных или функциональности (например, сбой загрузки службы при запуске).
Предупреждение	События, которые в момент записи в журнал не были существенными, но могут привести к сложностям в будущем (например, если на диске осталось мало свободного места).
Уведомление	Событие, описывающее удачное завершение действия приложением, драйвером или службой.
Аудит успехов	Событие, соответствующее успешно завершенному действию, связанному с поддержкой безопасности системы.
Аудит отказов	Событие, соответствующее неудачно завершенному действию, связанному с поддержкой безопасности системы. Вместе с «Аудитом успехов» единственные типы событий, регистрируемые в журнале безопасности.

В каждой записи аудита содержится информация, которая специфична для определенной категории контролируемого события. Описание данной информации представлено ниже.

Таблица 6.3 – Категории контролируемых событий

№ п/п	Категория события	Описание
1	Системное событие	Записи аудита дополнительно включают информацию о событиях относительно самой системы (например, очистка журналов аудита).
2	Доступ к объекту или службе каталогов	Записи аудита дополнительно включают информацию относительно имени объекта и затребованного вида доступа.
3	Использование привилегий	Записи аудита дополнительно идентифицируют привилегии субъекта.
4	Отслеживание процессов	Записи аудита дополнительно содержат информацию об идентификаторе процессов.
5	Изменение политики и управление учетной записью	Записи аудита дополнительно включают информацию о новых параметрах политики и, соответственно, измененных атрибутах учетной записи.
6	Вход в ОО с учетной записью или события входа в ОО	Записи аудита дополнительно включают информацию о причинах неуспешной попытки входа в ОО.
7	Вход в ОО	Запись аудита включает дополнительную информацию относительно типа входа пользователя в ОО: – интерактивный (локальный вход в ОО); – сетевой (вход через сеть); – в качестве службы; – в качестве пакетного задания.

В рамках ФБО определены две компоненты, выполняющих сбор данных о событиях аудита безопасности. На монитор безопасности SRM (Security Reference Monitor) возложена функция генерации данных аудита событий доступа к объекту,

использования привилегий и отслеживания процессов. Генерация данных аудита событий безопасности для всех остальных категорий реализуется службами, функционирующими совместно со службой LSA (Local Security Authority). Единственным исключением из данных правил является случай самостоятельной регистрация службой Event Logger события очистки журнала 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 службы LSA. Таким образом, администраторы устанавливают политику аудита, выбирая те или иные категории подвергаемых аудиту событий.

Другим компонентом ФБО, использующим политику аудита, является монитор безопасности SRM, контролирующий события доступа к объектам, использования привилегий и отслеживание процессов. Служба LSA и монитор безопасности SRM взаимодействуют через локальный порт подключения (local connection port), который используется для передачи параметров политики аудита монитору SRM. В случае изменения администратором политики аудита служба LSA актуализирует собственную базу данных и уведомляет об изменениях монитор безопасности SRM. Монитор безопасности SRM получает управляющий флаг, указывающий, что аудит разрешен, и структуру данных, определяющую категорию событий, подвергаемых аудиту.

В рамках каждой категории событий 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.

ФБО способны отслеживать и регистрировать события аудита, соответствующие определенным категориям, описание которых представлено ниже (см. таблицу 6.4). Перечень подвергаемых аудиту событий представлен в таблице 5.2. Каждой категории

событий в таблице 6.4 сопоставлены ассоциированные с определенными функциональными требованиями события аудита (их перечень приведен в таблице 5.2).

Таблица 6.4 – Регистрация событий по категориям.

№ п/п	Категория события	Описание	Компоненты согласно FAU_GEN.1
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).	FAU_STG.3, FAU_STG.4, FMT_MTD.1(1), FPT_AMT.1, FPT_TST.1
2.	Доступ к объекту	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.	FDP_ACF.1, FMT_MSA.1 (1), FMT_MSA.3 (1), FMT_REV.1(2)
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.	FMT_SMR.1, FPT_STM.1, FMT_MTD.1(8), FMT_MOF.1 (1), FMT_MTD.1(1), FAU_SAR.1, FAU_SAR.2
4.	Отслеживание процессов	Аудит событий, связанных с запуском, выполнением или прекращением работы каких-либо сервисов или приложений.	FIA_USB.1, FDP_ACF.1

№ п/п	Категория события	Описание	Компоненты согласно FAU_GEN.1
5.	Изменение политики	Аудит событий, связанных с изменением параметров и настроек политик безопасности, прав доступа на выполнение общесистемных операций и изменением режимов работы самой системы аудита.	FMT_MTD.1(2), FMT_MTD.1(3), FMT_REV.1(1), FMT_SMR.1, FMT_MOF.1 (1), FMT_MTD.2, FAU_GEN.1, FAU_SEL.1
6.	Управление учетной записью	Аудит событий, связанных с созданием, удалением или изменением учетных записей пользователей или групп, а также изменением их атрибутов.	FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5) FMT_REV.1(1), FMT_SAE.1, FMT_SMR.1, FIA_AFL.1
7.	Доступ к службе каталогов	Аудит событий доступа к объектам службы каталогов и соответствующим атрибутам данных объектов.	FDP_ACF.1
8.	Вход в систему с учетной записью	Аудит событий, связанных с регистрацией пользователей в ОО, в случае, когда контроллер домена получил запрос на проверку правильности учетной записи пользователя.	FIA_SOS.1, FIA_UAU.2, FIA_UID.2,

№ п/п	Категория события	Описание	Компоненты согласно FAU_GEN.1
9.	Вход в систему	Аудит событий, связанных с входом/выходом пользователя в/из системы, попытками установить сетевое подключение.	FIA_SOS.1, FIA_UAU.2, FIA_UID.2, FIA_AFL.1, FIA_USB.1, FTA_SSL.1, FTA_SSL.2, FTA_TSE.1, FTP_TRP.1

ФБО обеспечивают возможность ведение журнала безопасности брандмауэра Windows, в журнале регистрируются все успешные попытки подключения, которые осуществлялись через ОО, и подключения, которые были блокированы брандмауэром.

Журнал безопасности брандмауэра Windows состоит из следующих разделов:

– заголовка журнала – содержит сведения о версии журнала безопасности и о полях, которые доступны для ввода данных (см. таблицу 6.5);
– тела журнала – содержит полный отчет обо всей собранной и записанной информации о сетевом трафике или попытках подключения через ОО (см. таблицу 6.6).

Таблица 6.5 – Структура заголовка журнала безопасности брандмауэра Windows.

Элемент	Описание
#Version:	Версия установленного журнала безопасности.
#Software:	Имя журнала безопасности.
#Time:	Задает использование местного времени при записи в журнал отметок времени.
#Fields:	Статический список полей, доступных для записей журнала безопасности при наличии данных.

Таблица 6.6 – Структура тела журнала безопасности брандмауэра Windows

Поле	Описание
Дата	Год, месяц и день, когда произошла записанная транзакция. Дата представляется в следующем формате: ГГ-ММ-ДД, где ГГГГ - год, ММ - месяц, а ДД – число.
Время	Время, когда произошла записанная транзакция, записываемое в формате: ЧЧ:ММ:СС, где ЧЧ - часы в 24-часовом формате, ММ - минуты, а СС – секунды.
Действие	Операция, обнаруженная и зарегистрированная ОО. Могут записываться следующие действия: OPEN (открытие), CLOSE (закрытие), DROP (отклонение) и INFO-EVENTS-LOST (потерянные события). Для действия INFO-EVENTS-LOST указывается число событий, которые произошли, но не были записаны в журнал.
Протокол	Протокол, использовавшийся для передачи данных. Если протокол отличен от TCP, UDP и ICMP, в этом поле указывается число пакетов.
src-ip	IP-адрес источника (IP-адрес компьютера, пытавшегося установить подключение).
dst-ip	IP-адрес назначения (IP-адрес компьютера, с которым исходный компьютер пытался установить связь).
src-port	Номер порта источника – компьютера-отправителя. Правильное значение для параметра src-port определяется только для протоколов TCP и UDP. Номер порта задается целым числом в диапазоне от 1 до 65 535. Для всех остальных протоколов запись src-port отображается в виде «-» (дефис).
dst-port	Номер порта конечного компьютера. Правильное значение для параметра dst-port определяется только для протоколов TCP и UDP. Номер порта задается целым числом в диапазоне от 1 до 65 535. Для всех остальных протоколов запись dst-port отображается в виде «-» (дефис).
size	Размер пакета в байтах.
tcpflags	Флаги управления TCP, содержащиеся в заголовке TCP пакета IP: – **A**ck Acknowledgment field significant (включение поля подтверждения);

Поле	Описание
	– **F**in No more data from sender (конец массива данных отправителя); – **P**sh Push Function (функция принудительной доставки); – **R**st Reset the connection (сброс подключения); – **S**yn Synchronize sequence numbers (синхронизация порядковых номеров); – **U**rg Urgent Pointer field significant (включение поля указателя срочных данных). Флаги записываются прописными буквами.
tcpsyn	Последовательность портов TCP в пакете.
tcpack	Номер подтверждения TCP в пакете.
tcpwin	Размер окна TCP в байтах в пакете.
icmptype	Число, которое представляет поле Type (Тип) сообщения ICMP.
icmpcode	Число, которое представляет поле Code (Код) сообщения ICMP.
info	Сведения, зависящие от типа случившегося действия.

6.1.1.2 Просмотр журналов аудита

Инструментальное средство «Просмотр событий» (Event Viewer) предоставляет пользовательский интерфейс для просмотра содержимого журнала безопасности, а также возможность поиска и фильтрации конкретных событий. 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.

Просмотр журнала безопасности брандмауэра Windows осуществляется с помощью любого текстового редактора.

6.1.1.3 Защита журнала аудита от переполнения

ФБО предотвращают потерю данных аудита посредством управления регистрацией и очередью событий аудита. Исходя из настроек ОО, данные аудита добавляются в журнал 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 будет осуществляться вручную) или завершение работы в случае переполнении журнала аудита безопасности. При такой конфигурации, в случае завершения работы ОО в результате переполнения журнала аудита 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.

Как указывалось ранее, ФБО обеспечивают сбор информации о событиях аудита безопасности посредством монитора безопасности SRM и службы LSA. Оба компонента поддерживают очереди событий аудита. Монитор безопасности SRM помещает записи аудита во внутреннюю очередь для последующей их передачи службе LSA. Служба LSA поддерживает вторую очередь, которая содержит в себе данные аудита, переданные монитором SRM и другими службами. Обе очереди событий аудита отслеживают возможную потерю данных аудита. Служба SRM определяет верхнюю и нижнюю метку для собственной очереди событий аудита, что позволяет отследить момент ее заполнения. Служба LSA также поддерживает метки для собственной очереди событий аудита с целью определения момента ее заполнения.

Потеря данных аудита может произойти в случае, если очереди LSA и SRM достигнут установленных для них значений верхних меток либо в случае, когда размер файла журнала аудита безопасности достигнет своего предела. ОО может быть настроен таким образом, чтобы обеспечить аварийное завершение работы в случае заполнения журнала аудита. Размер файла журнала аудита безопасности может быть ограничен только размером ресурсов (объемом доступного дискового пространства), доступных в системе.

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 определен в роли уполномоченного администратора. Журнал безопасности является системным ресурсом, создаваемым на этапе установки системы. ОО не располагает интерфейсами, позволяющими создавать, удалять или изменять журнал аудита событий

безопасности. Подсистема безопасности LSA является единственной службой, обеспечивающей запись событий в журнал аудита безопасности.

Доступ к журналу безопасности брандмауэра Windows ограничивается механизмами дискреционной политики управления доступом.

Сопоставление с ФТБ

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

- FAU_GEN.1 – ОО обеспечивает генерацию данных аудита для всех категорий событий, представленных в таблице 6.4. Для каждого события аудита ФБО регистрируют дату, время, идентификатор пользователя или его имя, идентификатор события, источник, тип и категорию события;
- FAU_GEN.2 – все записи аудита включают идентификатор безопасности пользователя, уникально идентифицирующий пользователя;
- FAU_SAR.1 – инструментальные средства просмотра событий предоставляют администратору ОО возможность просмотра данных аудита в удобочитаемом формате;
- FAU_SAR.2 и FMT_MTD.1(1) – только администратору ОО предоставлены все виды доступа к журналу аудита;
- FAU_SAR.3 – ОО обеспечивает возможность выбора для заданной категории типа событий, подвергаемых аудиту («Аудит успехов» или «Аудит отказов»). Для категории событий доступа к объекту критерием выбора может являться идентификатор пользователя. ФБО определяют перечень подвергаемых аудиту событий на основе текущей конфигурации политики аудита и параметров, определяемых через списки назначений аудита. Инструментальные средство просмотра событий аудита предоставляют возможность выполнения поиска и фильтрации данных аудита по дате, времени, идентификатору безопасности и имени пользователя, имени компьютера, коду, источнику, типу и категории события;
- FAU_SEL.1 – ФБО предоставляют возможность включать события, потенциально подвергаемые аудиту, в совокупность событий, подвергающихся аудиту;

– FAU_STG.1 – интерфейс взаимодействия с журналом безопасности предоставляется службой «Регистратор событий». Только уполномоченные администраторы могут просматривать журнал аудита событий безопасности;
– 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;
– FMT_MTD.1(11) – ФБО предоставляют возможность устанавливать размер журнала аудита безопасности только администратору ОО;
– FAU_STG.4 – ОО может быть сконфигурирован на выполнение процедуры аварийного завершения в случае переполнения журнала аудита безопасности. После этого, только администратор ОО может выполнить регистрацию в ОО с целью очистки журнала аудита безопасности и возврата системы в рабочее состояние.

6.1.2 Функции безопасности ОО «Защита данных пользователя»

К предоставляемым ОО механизмам обеспечения защиты данных пользователя относятся:

– дискреционное управление доступом;
– 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 несколькими потоками, выполняющимися от имени пользователей. В таблице 6.7 представлен перечень объектов данных пользователя, на которые распространяется политика дискреционного управления доступом, устанавливаемая для ОО.

Таблица 6.7 – Перечень объектов, на которые распространяется политика дискреционного управления доступом.

№ п/п	Именованные объекты	Описание
1	Рабочий стол (Desktop)	Основной объект, используемый графическими дисплеями. По умолчанию службой WinLogon создается три рабочих стола.
2	Событие (Event)	Объект, создаваемый для механизма межпроцессного взаимодействия (IPC – Interprocess Communication).
3	Пара событий (Event Pair)	Объект, создаваемый для механизма межпроцессного взаимодействия.
4	Порт завершение I/O (I/O Completion Port)	Объект, обеспечивающий способы синхронизации I/O.
5	Задание (Job)	Объект, позволяющий управлять несколькими процессами как одним целым.
6	Ключ реестра (Registry Key)	Ключи реестра – это объекты, непосредственно формирующие сам реестр.
7	Мьютекс (Mutant)	Объект, создаваемый для механизма межпроцессного взаимодействия.
8	Каталог объектов (Object Directory)	Каталог в пространстве имен объектов.
9	Порт LPC (LPC port)	Объект механизма вызова локальных процедур.
10	Почтовый ящик (Mail slot)	Объект I/O, обеспечивающий передачу сообщений IPC через сеть.
11	Именованный канал (Named Pipe)	Объект I/O, используемый для обеспечения межпроцессного взаимодействия через сеть.
12	Каталог NTFS (NTFS Directory)	Объект файловой системы NTFS.
13	Файл NTFS (NTFS file)	Файл данных пользователя, управляемый NTFS.
14	Принтер (Printer)	Представление конкретной очереди печати и всех соответствующих ей устройств печати.

№ п/п	Именованные объекты	Описание
15	Каталог AD (Active Directory)	Представление общих ресурсов, определяемых и поддерживаемых службой AD.
16	Процесс (Process)	Потоки, выполняющиеся в едином контексте и имеющие общее адресное пространство и память.
17	Секция (Section)	Область памяти.
18	Семафор (Semaphore)	Объект, создаваемый для механизма межпроцессного взаимодействия.
19	Символьная ссылка (Symbolic Link)	Способ обеспечения альтернативного именования в пространстве имен объекта.
20	Поток (Thread)	Поток – это контекст выполнения (например, набор регистров, стеков). Все потоки в пользовательском режиме ассоциированы с процессами.
21	Таймер (Timer)	Механизм, позволяющий потоку осуществлять задержку исполнения на указанное время.
22	Маркеры (Tokens)	Данные объекты представляют контекст безопасности процессов или потоков.
23	Том (Volume)	Один или несколько разделов, отформатированных для использования файловой системой.
24	Объект «Window Station»	Контейнер для объектов рабочего стола и связанных с ними атрибутов.

Атрибуты субъектов дискреционного управления доступом

Маркеры содержат набор атрибутов безопасности для каждого субъекта. Маркеры ассоциируются с каждым процессом или потоком, выполняемым от имени определенного пользователя. В маркере содержится следующая информация:

– идентификатор безопасности (SID – Security Identifier) пользователя;
– идентификаторы безопасности соответствующих групп, членами которых является данный пользователь;

– назначенные пользователю привилегии;
– устанавливаемый по умолчанию дискреционный список управления доступом (для создаваемых объектов);
– идентификатор безопасности владельца;
– тип маркера (основной или имперсонированный);
– уровень имперсонации (для имперсонированных маркеров);
– идентификатор сеанса.

Для потока может быть определен имперсонированный маркер доступа, который используется вместо маркера родительского процесса при выполнении процедуры контроля доступа и генерации данных аудита в контексте безопасности другого субъекта. В результате данный поток имперсонирует (олицетворяет) субъекта, предоставившего данный вид маркера доступа. Механизм имперсонации прекращает действовать, когда имперсонированный маркер удаляется из потока или при завершении потока.

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

Атрибуты объектов дискреционного управления доступом

Дескрипторы безопасности содержат все атрибуты безопасности, ассоциированные с объектом. К атрибутам безопасности, содержащимся в дескрипторе безопасности, относятся:

– идентификатор безопасности владельца объекта;
– дискреционный список управления доступом, содержащий информацию о разрешениях и запретах, установленных для данного объекта;
– системный список управления доступом SACL, содержащий строки назначений аудита.

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

– идентификатор безопасности пользователя и группы;
– разрешения, предоставленные определенному пользователю или группе;
– значения разрешений (разрешить/запретить).

Каждая запись ACE содержит атрибуты наследования, определяющие иерархию объектов, к которым будут применены установленные права доступа, т.е. область применения данных прав доступа может охватывать только данный объект, только дочерние объекты или те и другие.

Существуют два типа строк управления доступом:

1. ALLOW ACES – разрешающие:

ACCESS_ALLOWED_ACE – используется для назначения доступа пользователям или группе пользователей;

ACCESS_ALLOWED_OBJECT_ACE - используется для назначения доступа пользователям или группе пользователей к отдельным атрибутам объектов службы каталогов AD, либо для ограничения наследования записей ACE для определенных типов дочерних объектов. Данный тип записей ACE поддерживается только для объектов службы каталога AD.

2. DENY ACES – запрещающие:

ACCESS_DENIED_ACE - используется для запрета доступа пользователям или группе пользователей;

ACCESS_DENIED_OBJECT_ACE - используется для запрета доступа пользователям или группе пользователей к отдельным атрибутам объектов службы каталогов AD, либо для ограничения наследования записей ACE для определенных типов дочерних объектов. Данный тип записей ACE поддерживается только для объектов службы каталога AD.

Маска доступа определяет назначенные (или запрещенные) с привязкой к конкретному идентификатору безопасности пользователя или группы пользователей права доступа. Маска доступа 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. 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. ФБО ассоциируют маску назначенного доступа с каждым открытым описателем. 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, ФБО 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

ФБО реализуют 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 представляет краткое описание механизма принятия решения о разрешении доступа к объекту данных пользователя. Для того, чтобы предоставить доступ к объекту, необходимо выполнить проверку прав доступа, указанных в маске запрашиваемого доступа. Проверка прав выполняется по шагам в порядке следования записей 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. **Проверка привилегий**

Проверка привилегии SeSecurityPrivilege – данная проверка необходима, если привилегия ACCESS_SYSTEM_SECURITY присутствует в маске запрашиваемого доступа. Если запрашивающему субъекту необходима привилегия ACCESS_SYSTEM_SECURITY, но таковой у него нет, то доступ будет запрещен. В противном случае полномочия будут предоставлены.

Проверка привилегии SeTakeOwnerPrivilege – если в маске запрашиваемого доступа присутствует право доступа WRITE_OWNER и маркер доступа запрашивающего субъекта содержит привилегию SeTakeOwnerPrivilege, тогда право доступа WRITE_OWNER предоставляется.

2. **Проверка Владельца (Owner)**

Проверка всех идентификаторов безопасности, указанных в маркере доступа, с целью определения совпадения с идентификатором безопасности владельца объекта. Если совпадение найдено, то при необходимости могут быть предоставлены права доступа READ_CONTROL и WRITE_DAC.

3. **Дискреционный список управления доступом отсутствует**

В дальнейшем все требуемые права доступа будут предоставлены.

4. **Дискреционный список управления доступом представлен, но не содержит записей**

Если запрашиваются какие-либо дополнительные права доступа, в доступе будет отказано.

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

Если атрибуты наследования указывают, что областью применения данной записи ACE 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 совпали и маска доступа, представленная в ACE, соответствует маске запрашиваемого доступа:

- **разрешающие записи ACE** – если тип записи ACE является ACCESS_ALLOWED_OBJECT_ACE (т.е. в данной записи представлены разрешающие права доступа) и запись ACE включает идентификатор GUID, отождествляемый с атрибутом соответствующего объекта, в таком случае доступ будет предоставлен к данному атрибуту, а не ко всему объекту в целом, в противном случае доступ предоставляется ко всему объекту;
- **запрещающие записи ACE** – если тип записи ACE является ACCESS_DENIED_OBJECT_ACE (т.е. в данной строке представлены права запрещающие доступ) и запись ACE включает идентификатор GUID, отождествляемый с атрибутом соответствующего объекта, в таком случае доступ к данному атрибуту будет запрещен, В противном случае доступ будет запрещен ко всему объекту; если для запрашиваемого доступа задан явный запрет через запись ACE, тогда дальнейшая проверка прав доступа будет прекращена.

Обеспечение защиты через устанавливаемые по умолчанию права доступа

ФБО обеспечивают применение устанавливаемых по умолчанию прав доступа ко всем создаваемым объектам. При создании новых объектов для них определяется соответствующий дискреционный список управления доступом одним из следующих методов:

- если при создании объекта явно указывается дескриптор безопасности (как часть запроса на создание), в таком случае список DACL формируется на основе предоставленного дескриптора безопасности;
- если дескриптор безопасности не представлен как часть запроса на создание объекта, список DACL формируется, на основе списка DACL родительского объекта только в том случае, если представленные в нем записи ACE имеют

соответствующие атрибуты наследования, указывающие, что область их применения охватывает все дочерние по отношению к данному объекты;

– если не существует родительского объекта, от которого можно унаследовать записи ACE, то список DACL будет формироваться, основываясь на установленном по умолчанию списке DACL в маркере доступа субъекта.

Для всех маркеров доступа определяется соответствующий устанавливаемый по умолчанию список DACL, который будет применяться ко всем создаваемым объектам.

6.1.2.2 Фильтрация информации

ФБО обеспечивают защиту персонального компьютера, непосредственно подключенного к сети, или персональных компьютеров и устройств, подключенных к компьютеру, через который осуществляется общий доступ к подключению к сетям общего доступа, 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 firewall), 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.

ФБО обеспечивают защиту персонального компьютера от сетевых атак на время запуска и выключения ОО, что обеспечивает дополнительную безопасность с момента включения компьютера до момента его выключения. Используемая на данном этапе политика *boot-time policy* является неизменяемой и определяется параметрами, позволяющими ОО на этапе загрузки или выключения осуществлять сетевое взаимодействие только по протоколам DHCP и DNS и подключаться к контроллеру домена для получения параметров групповой политики.

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 персонального 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 персонального компьютера. В противном случае сеансы связи, инициируемые из источников, находящихся с внешней стороны персонального 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;
- выводит диалоговое окно, запрашивающее пользователя о необходимости блокирования или разрешения подключения;
- разрешает подключение.

Поведение ФБО определяется списком исключений, задаваемых для программ и портов, которые могут определяться централизованно через объекты групповой политики, применяемые для компьютера, или 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 или запрещается получение незапрашиваемых входящих запросов по любому порту, которые они пытаются открыть, даже если указанный порт заблокирован с использованием другой политики. Таким образом, в случае, если указанный порт заблокирован с использованием политики «Брандмауэр Windows: Задать исключения для портов» программа, которая включена в список исключений и разрешена, сможет получать входящие сообщения, адресованные ей. 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 если приложение включено в список исключений для программ и запрещено, оно не сможет открыть требуемый порт. Если приложение не включено в список исключений для программ, то при попытке открыть порт на экран будет выведено сообщений, информирующее пользователя о данном факте и предлагающее ему, при наличие у последнего необходимых прав, выполнить одно из следующих действий:

- разблокировать приложение, что фактически означает помещение его в список исключений для программ, которым разрешено открывать порт;
- блокировать работу приложения, что фактически означает помещение его в список исключений для программ с параметром, определяющим запрет на открытие портов компьютера.

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. Таким образом, ФБО предоставляют программам и службам возможность взаимодействовать через вычислительную сеть без ограничений и ущерба для их функциональности.

При задании списка исключений для портов или программ ФБО обеспечивают возможность задания области действия данных исключений, определяемой диапазоном IP-адресов персональных компьютеров, на которых они распространяются и для которых указанные порты и программы разблокированы.

ОО поддерживает следующие режимы функционирования ФБО:

- *включен* – ФБО блокирует все внешние запросы к персональному компьютеру, кроме запросов программ и служб, определяемых с использованием политики исключения;
- *включен без исключений* – при определении параметра «*Не позволять исключения*» ФБО блокируют все внешние запросы на соединение с персональным компьютером, включая запросы программ и служб, перечисленных на вкладке исключений. Данный режим функционирования

ФБО используется в случае необходимости обеспечения максимальной защищенности компьютера от возможных сетевых атак;

– *выключен* – данный режим функционирования используется в случае, если защита клиентского компьютера осуществляется с использованием брандмауэра сторонних производителей.

6.1.2.3 Защита остаточной информации

ФБО обеспечивают недоступность предшествующего информационного содержания ресурсов при распределении их субъектам и объектам. ФБО гарантируют, что ресурсы, выделяемые процессам в пользовательском режиме, не имеют остаточной информации, и процессы не смогут прочитать или восстановить их содержимое.

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.

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

- FDP_ACC.1 – монитор безопасности SRM выступает в качестве посредника при всех обращениях к объектам, в том числе к объектам в режиме ядра (привилегированный режим) и в пользовательском режиме (непривилегированный режим). Механизм предоставления доступа к объектам основывается на проверке монитором безопасности SRM достоверности запрашиваемого доступа. Для большинства объектов данная процедура заключается в проверке прав при инициировании доступа и дальнейшем использовании объекта через описатели, которые включают маску назначенного доступа;
- FDP_ACF.1 – ФБО обеспечивают доступ к объектам, основываясь на использовании маркеров доступа, содержащих идентификаторы безопасности и перечень привилегий, назначенных субъектам, и дескрипторах безопасности объектов. 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;
- FMT_MSA.1 (1) – возможность изменять политику дискреционного управления доступом контролируется посредством полномочий на изменение списков дискреционного управления доступом. Ниже представлено четыре механизма, посредством которых контролируются изменения в списках DACL:
  - *Владелец объекта*: имеет явное право WRITE_DAC на изменение списка DACL;
  - *Явное право изменять список DACL*: пользователю явно назначается право WRITE_DAC на изменение списка DACL;

  - *Право смены владельца*: пользователь с явно назначенным правом WRITE_OWNER на список DACL может сменить владельца данного объекта и в последующем использовать явное право WRITE_DAC, предоставляемое владельцу объекта по умолчанию;
  - *Использование привилегии «Смена владельца»*: пользователь с привилегией SeTakeOwnerPrivilege может сменить владельца данного объекта и в последующем использовать явное право WRITE_DAC, предоставляемое владельцу объекта по умолчанию;
- FMT_MSA.3 (1) – 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_MSA.1 (2) – ФБО предоставляют возможность модифицировать значения атрибутов безопасности в правилах фильтрации входящих информационных потоков только администратору ОО;
- FMT_MSA.1 (3) – ФБО предоставляют возможность модифицировать правила фильтрации входящих информационных потоков только администратору ОО;
- FMT_MSA.3 (2) – ФБО устанавливают запрет на все входящие информационные потоки по умолчанию при инициализации брандмауэра Windows, только администратору ОО доступны возможности по дальнейшей модификации политики фильтрации;
- FMT_REV.1 (2) – возможность отзывать права доступа к объекту управляется через наличие полномочий изменять список DACL и регулируется теми же условиями, которые были изложены ранее в FMT_MSA.1;
- FDP_RIP.2 – ФБО обеспечивают недоступность предыдущего информационного содержания ресурсов при их перераспределении для новых объектов. Данная возможность реализуется через обнуление или перезаписывание страниц памяти и отслеживание указателей чтения/записи для дисковой памяти.

6.1.3 Функции безопасности ОО «Идентификация и аутентификация»

ОО 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 вход в 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 определенным требованиям.

6.1.3.1 Типы входа в ОО

ОО поддерживает четыре типа входа пользователя:

- интерактивный – локальный вход пользователя в ОО;
- сетевой – вход в ОО через сеть;
- вход в качестве службы;
- вход в качестве пакетного задания.

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

Для каждого типа входа определено соответствующее право, которое должно быть назначено учетной записи пользователя и группе пользователей с целью возможности контроля доступных пользователю способов регистрации в ОО.

Доверенный маршрут

С целью защиты идентификационной и аутентификационной информации при первоначальном интерактивном входе пользователя в ОО необходимо обеспечить ее передачу через доверенный маршрут. Доверенный маршрут вызывается одновременным нажатием клавиш Ctrl+Alt+Del, что всегда фиксируется ФБО, т.е. данное действие не может быть прервано или перехвачено недоверенным процессом. Для получения информации от пользователя задействуются служба WinLogon и модуль Graphical Identification and Authentication (GINA). Основная задача модуля GINA - сбор идентификационной и аутентификационной информации, вводимой пользователем, и передача ее в строго определенном формате модулю LSA. Модуль GINA предоставляет интерфейс с устройством, через которое пользователь регистрируется в системе (в частности стандартное диалоговое окно входа в систему).

6.1.3.2 База данных атрибутов пользователя

Описание учетных записей пользователей и групп

ФБО поддерживают базу данных, в которой полностью определены учетные записи пользователей и групп. Каждая учетная запись представлена в данной базе набором атрибутов:

- *имя учетной записи* – используется для представления учетной записи в удобочитаемой форме;
- *идентификатор безопасности SID* – идентификатор используется 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;
- *группы* – используются, 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 вход в систему* – право, присвоенное пользователю и определяющее способы его входа в систему;

– *управляющая информация* – используется, чтобы контролировать дополнительные относящиеся к безопасности атрибуты 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 зависит от среды функционирования ОО, которая определяется конфигурациями Enterprise, High Security и Stand-Alone.

Если среда функционирования определена как Stand-Alone, в этом случае ОО будет поддерживать собственную базу данных учетных записей пользователей и групп, которые будут описаны одной совокупностью атрибутов. В случае функционирования ОО в среде Enterprise или High Security, совокупность атрибутов будет значительно расширена.

Политики учетных записей

Политика учетных записей может быть определена отдельно для ОО (в случае если среда функционирования определена как Stand-Alone) либо централизовано для всех ОО (в случае их функционирования в среде Enterprise или High Security). Политика учетных записей определяется и управляется уполномоченным администратором. Через политику учетных записей можно задать политику блокировки учетной записи и политику паролей.

Политика паролей включает:

– максимальный срок действия пароля;
– минимальная длина пароля;
– минимальный срок действия пароля;
– требование соответствия пароля требованиям сложности;
– требование неповторяемости паролей.

Политика блокировки учетной записи позволяет задать:

– временной интервал блокировки учетной записи;
– пороговое значение блокировки;

– временной интервал, после которого произойдет сброс счетчика блокировки.

Данные политики позволяют ФБО реализовывать единый механизм безопасности для всех пользователей, осуществлять централизованное управление без необходимости управления каждым из них в отдельности. Например, ФБО автоматически потребуют смену пароля для каждого пользователя по истечению максимального срока действия пароля. Таким же образом, при достижении порогового значения ошибок входа в ОО учетная запись пользователя будет заблокирована и в последующем разблокирована через установленный интервал времени.

6.1.3.3 Процесс входа в ОО

Все запросы на вход в ОО обрабатываются одним и тем же способом, независимо от их типа (интерактивный, сетевой вход в систему, вход 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 среде Enterprise или High Security.

Ключевым модулем служб аутентификации является Local Security Authority (LSA), который выполняет роль диспетчера.

Модель аутентификации 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 диспетчеру LSA при старте ОО. Пользователь, запрашивающий аутентификацию по какому-либо протоколу, передает свои параметры диспетчеру LSA, который вызывает соответствующий пакет аутентификации и передает ему эти параметры. При успешной проверке именно пакет аутентификации инициирует новый пользовательский сеанс и формирует список идентификаторов безопасности, который затем будет включен в маркер доступа аутентифицированного пользователя.

В составе ОО поставляются два пакета аутентификации:

– пакет, обеспечивающий локальную аутентификацию и поддержку протокола NTLM;
– пакет Kerberos, реализующий поддержку протокола Kerberos, являющегося основным протоколом аутентификации.

Интерактивная локальный вход пользователя

1. Аутентификация начинается с явного запроса системой у пользователя его регистрационных данных. Для получения информации от пользователя задействуются служба WinLogon и модуль Graphical Identification and Authentication (GINA). Основная задача GINA – сбор информации, введенной пользователем, и передача ее в строго определенном формате модулю LSA.

2. Диспетчер LSA обрабатывает запрос и посылает его в формате пакета аутентификации Kerberos службе Kerberos (поскольку протокол аутентификации Kerberos используется по умолчанию).

3. В ответ на этот запрос служба Kerberos возвращает сообщение об ошибке, поскольку данный пакет предназначен для аутентификации не локальных, а доменных пользователей.

4. Диспетчер LSA получает это сообщение об ошибке и возвращает его GINA.

5. GINA повторно посылает запрос с указанием пакета аутентификации NTLM.

6. Если аутентификационные данные совпали и учетная запись верна – происходит локальный вход в систему.

Интерактивный вход в домен (при функционировании ОО в среде Enterprise или High Security)

1. Получив запрос на вход в ОО, модуль LSA передает его в формате пакета аутентификации Kerberos службе Kerberos, сообщая ей имя пользователя и имя домена (запрос на получение билета TGT).

2. Kerberos инициирует AS-ответ (AS – Authentication Service), содержащий билет TGT (Ticket-Granting Ticket – «билет на получение билета») и отсылает его клиенту. В составе билета TGT включен идентификатор безопасности учетной записи и всех групп, в

которые входит данный пользователь. Однако успешная аутентификация пользователя не означает, что пользователь получает разрешение на доступ к ресурсам рабочей станции.

3. Далее клиент посылает запрос службе Ticket Granting Service (TGS), содержащий полученный билет TGT, чтобы получить доступ на локальный компьютер.

4. Служба Kerberos генерирует и посылает ответ от службы Ticket Granting Service. Он содержит билет на рабочую станцию. В данном билете содержатся идентификатор безопасности учетной записи и всех глобальных групп, скопированных службой Kerberos с оригинального 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 локальным 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. Kerberos, напротив, требует, чтобы запрос на вход был частично преобразован с помощью хэшированного пароля. Преобразованный запрос пересылается соответствующему контроллеру домена, который в свою очередь ищет хэшированный 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 вход 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.

Если нет никаких ограничений, которые могут повлиять на успешный вход пользователя в ОО, происходит формирование процесса, опосредованно представляющего пользователя при его работе с ресурсами информационной системы, и назначение данному процессу маркера доступа, который определяет контекст безопасности, в рамках которого будет функционировать процесс.

6.1.3.4 Имперсонация

В некоторых случаях, особенно при организации клиент-серверного взаимодействия, существует необходимость обеспечить взаимодействие потока, выполняемого в рамках процесса, которому передан первичный маркер доступа одного пользователя, с объектом в контексте безопасности другого. Для реализации данного механизма ФБО поддерживают возможность имперсонации клиента. Как описывалось выше, каждый процесс имеет первичный маркер доступа, включающий идентификатор безопасности пользователя, групп, привилегии, права на вход и устанавливаемый по умолчанию список DACL. Обычно, каждый поток, выполняемый в рамках какого-либо процесса, использует маркер доступа процесса, который таким образом определяет его контекст безопасности. Однако, поток может иметь два маркера доступа: первичный и имперсонированный маркер доступа, который будет использоваться вместо первичного маркера доступа процесса для организации взаимодействия с объектом в контексте безопасности другого пользователя. Данный механизм актуален, например, для распределенных приложений (COM+). Допустим, клиент зарегистрировался в сети и запустил некое приложение. Это приложение, в свою очередь, пытается активизировать какой-то компонент на другой машине. Для того, чтобы это сделать прозрачно, можно передать пользовательский билет самому приложению, с тем, чтобы оно на другой машине активизировалось в контексте пользователя, который был аутентифицирован.

Имперсонация прекращается при удалении имперсонированного маркера доступа или завершения потока, имеющего имперсонированный маркер доступа.

6.1.3.5 Стойкость аутентификации

Как указывалось выше, ФБО предоставляют 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 ОО «Идентификация и аутентификация» удовлетворяют следующим функциональным требованиям безопасности:

- FIA_AFL.1 – ФБО блокируют учетную запись пользователя после превышения установленного администратором порогового значения неуспешных попыток входа в систему. Учетная запись будет заблокирована до тех пор, пока администратор ОО не разблокирует ее или не истечет установленный интервал времени блокирования;
- 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, аутентификационной информацией, привилегиями, правами на вход и членством в группах, а также другой управляющей информацией;
- FIA_SOS.1 – использование сложных паролей уменьшает вероятность их подбора примерно до $2{,}5 \times 10^{14}$.
- FIA_UAU.2 – администратор ОО имеет возможность сконфигурировать ФБО таким образом, чтобы обеспечить аутентификацию до любых действий субъектов доступа;

- FIA_UAU.7 – с целью предотвращения раскрытия пароля субъекта доступа во время интерактивной аутентификации ФБО обеспечивают его отображение в виде символов «*»;
- FIA_UID.2 – администратор ОО имеет возможность сконфигурировать ФБО таким образом, чтобы обеспечить идентификацию до любых действий 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;
- FMT_MTD.1(10) – администратор ОО имеет возможность формировать предупреждающее сообщение при установлении сеанса пользователем;
- FTA_TAB.1 – ФБО обеспечивают отображение предупреждающего сообщения при установлении сеанса пользователем в случае, если оно сформировано администратором ОО;
- 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 вход в ОО (нажатие комбинации клавиш Ctrl-Alt-Del), который обеспечивает прямое взаимодействие пользователя с ФБО с целью передачи регистрационной информации и интерактивного входа в систему;
- FMT_SMR.3 – чтобы принять роль уполномоченного администратора, пользователь должен осуществить успешный вход в ОО с соответствующими привилегиями или являться членом административной группы.

6.1.4 Функции безопасности ОО «Управление безопасностью»

ОО поддерживает ролевую модель, а также 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 группы. При

осуществлении входа в 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: администратора ОО и пользователя ОО.

Роль 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 «Администраторы». Пользователю будут даны 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.

Любой субъект доступа, осуществивший вход в ОО и не выступающий в роли администратора ОО, рассматривается как пользователь ОО.

6.1.4.2 Функции управления безопасностью

ОО поддерживает набор политик и характеристик безопасности, которые требуют соответствующего управления. За некоторым исключением, функции по управлению безопасностью предоставлены только 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 администратору 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 аудита безопасности, а также администратор ОО 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 администратору ОО возможность устанавливать ограничения на применяемые пароли и определять параметры блокировки учетных записей. Определяя

политику использования паролей, 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 выполнить вход в ОО до того момента, пока не сменит пароль. Параметры блокировки учетных записей определяют пороговое значение неуспешных попыток входа, при превышении которого учетная запись будет заблокирована, продолжительность блокировки и интервал времени, после которого произойдет сброс счетчика блокировки.

База данных учетных записей пользователей – функции управления базой данных учетных записей позволяют администратору ОО управлять (определять, назначать и удалять) атрибутами безопасности учетных записей пользователей и групп. Каждая учетная запись описывается следующим 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. Администратор ОО при создании учетной записи пользователя определяет только начальный пароль, который в последствии может быть изменен как самим администратором ОО, 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 администратору ОО назначать или удалять для конкретных учетных записей пользователей или групп права входа в систему и определенные привилегии.

Дисковые квоты – функции управления дисковыми квотами позволяют администратору ОО управлять дисковыми квотами на томах NTFS. 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.

Очистка памяти – функции управления механизмами очистки памяти позволяют администратору ОО включать и выключать режим очистки содержимого файлов подкачки.

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

Тестирование оборудования и ФБО – функции управления тестированием оборудования и ФБО позволяют администратору ОО определять условия тестирования.

Фильтрация информации – функции управления фильтрации информации (реализуется брандмауэром Windows) позволяют администратору ОО формировать правила, на основании которых происходит управление входящими в ОО информационными потоками.

Сопоставление с ФТБ

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

- FMT_MOF.1 (1) – только администратор ОО может разрешать или запрещать политику аудита событий, выбирать категории событий, которые будут подвергнуты аудиту, указывать тип контролируемого события (успех/отказ), разрешать или запрещать процедуры очистки остаточной информации в файлах подкачки, управлять политикой фильтрации информации, назначать приоритеты процессам, упралять квотированием томов NTFS, определять условия тестирования оборудования и ФБО, управлять условиями открытия сеанса доступа;
- FMT_MOF.1 (2) – только администратор ОО и пользователь ОО могут управлять блокированием сеансов;
- FMT_MTD.1 (1) – только администратор ОО может создавать, удалять или очищать журнал аудита событий безопасности;
- FMT_MTD.1 (2) – только администратор ОО имеет доступ к журналу аудита событий безопасности;
- FMT_MTD.1 (3) – только администратор ОО может управлять учетными записями пользователей и групп, определять членство в группах, назначать привилегии и права доступа, а также определять другие относящиеся и не относящиеся к безопасности атрибуты (за исключением пароля, который может быть самостоятельно изменен пользователем);

- FMT_MTD.1 (4) – только администратор ОО может устанавливать начальный пароль для пользователя ОО;
- FMT_MTD.1 (5) – установленный администратором ОО начальный пароль может быть изменен только администратором ОО или уполномоченным пользователем ОО;
- FMT_MTD.1 (6) – только администратор ОО может изменять интервал продолжительности блокировки учетной записи;
- FMT_MTD.1 (7) – только администратор ОО может изменять минимальную длину пароля;
- FMT_MTD.1 (9) – только администратор ОО может управлять дисковыми квотами и определять действия, которые необходимо выполнить в случае превышения объема выделенных квот;
- FMT_MTD.2 – только администратор ОО может устанавливать и изменять максимальное число неуспешных попыток входа в ОО, после превышения которых, учетная запись пользователя будет заблокирована;
- FMT_REV.1(1) – только администратор ОО может отменять атрибуты безопасности, определенные для учетных записей пользователей и групп;
- FMT_SAE.1 – только администратор ОО может устанавливать параметры политики учетных записей, включая максимальный срок действия пароля;
- FMT_SMR.1 – ОО поддерживает ролевую модель, определяя роль администратора ОО через механизм назначения привилегий или добавлением учетной записи в соответствующую административную группу.

6.1.5 Функции безопасности ОО «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

ФБО обеспечивают изоляцию процессов и поддерживают 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 обеспечивает 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, храниться в защищенной памяти режима ядра.

Инструментальные средства администрирования реализуют функции управления в контексте безопасности процесса, запущенного от имени уполномоченного администратора. 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 с целью обеспечения непротиворечивости службы времени.

Сопоставление с ФТБ

Функции безопасности ОО «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 пользователя ОО;
- FPT_ITC.1 – ФБО позволяют обеспечить конфиденциальность передаваемой для аутентификации и авторизации на контроллере домена аутентификационной информации;
- FPT_RVM.1 – ФБО предоставляют посредничество при доступе к объектам через применение описателей;
- FPT_SEP.1 – ФБО предоставляют домен безопасности для собственной защиты посредством аппаратных средств, контролируемых переходов из одного состояния в другое, изоляцию процессов и защиту памяти;
- FPT_STM.1, FMT_MTD.1(8) – 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 предоставляют надежные метки времени для ФБО;
- FPT_TST.1 – ФБО осуществляют самотестирование в процессе запуска ОО и по требованию уполномоченного пользователя в процессе функционирования.

6.1.6 Функции безопасности ОО «Использование ресурсов»

ФБО предоставляют 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 администратором ОО. Данные свойства позволяют администратору ОО 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.

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, «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 администратором ОО действия.

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

Сопоставление с ФТБ

Функции безопасности ОО «Использование ресурсов» 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 квотирование на томах NTFS предоставляет 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»

ФБО предоставляют пользователям ОО возможность блокировать собственный интерактивный сеанс немедленно или по истечению определенного ими временного интервала. После того, как пользователь осуществил вход в ОО, он может заблокировать сеанс путем нажатия комбинации клавиш Ctrl-Alt-Del. Данная комбинации 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.

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 включиться 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 уполномоченным 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 нужно нажать комбинацию клавиш Ctrl-Alt-Del для повторного входа в ОО. Независимо то 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 локальной системой при первоначальной регистрации, после чего пользователь возвратиться в собственный сеанс.

С другой стороны, администратор ОО может ввести собственный идентификатор и пароль для входа в систему. Если ФБО успешно аутентифицируют администратора ОО, сеанс пользователя ОО, 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 определять период бездействия, по окончании которого его сеанс будет заблокирован. Для возврата в собственный сеанс пользователь ОО должен заново ввести свои идентификационные и аутентификационные данные;
- FTA_SSL.2 – ОО предоставляет пользователю ОО возможность самостоятельно блокировать сеанс;
- FMT_MOF.1 (2) – только уполномоченный пользователь ОО и администратор ОО могут разблокировать заблокированный сеанс;
- FMT_MTD.1(12) – ФБО позволяет уполномоченным пользователям ОО определять и изменять интервал бездействия до того как сеанс данного пользователя ОО будет заблокирован.

6.2 Меры доверия к безопасности ОО

Для удовлетворения требований доверия к безопасности согласно ОУД1 усиленному 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, связывающее 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

Корпорация Microsoft® предоставляет руководства безопасной установки, генерации и запуска. В процедурах установки, генерации и запуска описаны шаги,

необходимые для получения безопасной конфигурации ОО, описанной в ЗБ. Эти процедуры задокументированы в «Windows XP Security Guide».

Корпорация Microsoft® 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. Руководства администратора и пользователя задокументированы в «Windows XP 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

Тестовая документация ОО описывает стратегию тестирования ФБО, тестовые сценарии, наборы тестов и результаты тестирования, позволяющие провести независимое тестирование ФБО и сделать заключение, выполняются ли ФБО в соответствии со спецификациями.

Тестовая документация представлена в документах:

– «Testing the Windows XP Security Guide»;
– «Windows XP Security Guide Test Cases».

Оценщику предлагается использовать данную тестовую документацию как основу для выполнения тестов по отношению к ОО. Тестовая документация используется как основа для тестирования, но это не мешает оценщику разработать и выполнить новые тесты. Эти новые тесты записываются в тестовую документацию.

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 «Материалы анализа стойкости функций безопасности Microsoft® Windows® XP Professional Service Pack 3 Service Pack 1a».

Сопоставление с ТДБ

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

– AVA_SOF.1.

7 Утверждения о соответствии ПЗ

В этом разделе предоставляются утверждения о соответствии профилю защиты и приводится обоснование этих утверждений.

7.1 Ссылка на ПЗ

Объект оценки и его ЗБ соответствует профилю защиты «Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003».

7.2 Конкретизация ПЗ

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

Профиль защиты «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 (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 «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

Наименование требования	Изменение
FDP_ACF.1	завершено уточнено
FIA_AFL.1	завершено
FIA_ATD.1	завершено
FIA_SOS.1	уточнено
FIA_USB.1	завершено
FMT_MOF.1	завершено
FMT_MSA.1	завершено
FMT_MSA.3	завершено
FMT_REV.1 (1)	завершено
FMT_REV.1 (2)	завершено
FMT_SMR.1	завершено
FPT_AMT.1	завершено
FPT_TST.1	завершено
FTA_TSE.1	уточнено
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.

FIA_SOS.1 – уточнен относительно ПЗ в связи с особенностями реализации ОО.

FTA_TSE.1 – уточнен относительно ПЗ в связи с особенностями ОО – возможностью открытия сеанса, учитывая время доступа.

7.3 Дополнение ПЗ

В настоящее ЗБ включены следующие дополнительные политики безопасности организации, не вошедшие в ПЗ «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 удаленным доверенным системам ИТ.

P.Filtration – включена в связи с дополнительной возможностью ОО – осуществлением фильтрации входящих в ОО информационных потоков.

Добавленные в настоящее ЗБ политики безопасности организации не противоречат ПЗ.

В настоящее ЗБ включены следующие дополнительные цели безопасности, не вошедшие в ПЗ «Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003».

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

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

O.Filtration – ФБО должны располагать механизмами, осуществляющими фильтрацию входящих в ОО информационных потоков.

Включение данных целей безопасности связано с добавлением в ЗБ политик безопасности организации **P.Warn, P.Sec** и **P.Filtration**.

Добавленные в настоящее ЗБ цели безопасности не противоречат ПЗ.

В настоящее ЗБ включены следующие дополнительные функциональные требования, не вошедшие в ПЗ «Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003».

FDP_IFC.1 – включен в связи с дополнительной возможностью ОО – реализацией политики фильтрации информации.

FDP_IFF.1 – включен в связи с дополнительной возможностью ОО – использованием, при осуществлении фильтрации входящих в ОО информационных потоков, атрибутов безопасности субъектов и информации, а также правил осуществления фильтрации.

FMT_MTD.1 (6) – включен в связи с дополнительной возможностью ОО – установкой и модификацией уполномоченным администратором продолжительности блокировки учетной записи пользователя после превышения порога неуспешных попыток аутентификации.

FMT_MTD.1 (7) – включен в связи с дополнительной возможностью ОО – установкой и модификацией уполномоченным администратором минимально допустимой длины пароля.

FMT_MTD.1 (8) – включен в связи с дополнительной возможностью ОО – установкой и модификацией уполномоченным администратором представления времени ФБО.

FMT_MTD.1 (9) – включен в связи с дополнительной возможностью ОО – установкой и модификацией уполномоченным администратором квот на томах NTFS.

FMT_MTD.1 (10) – включен в связи с дополнительной возможностью ОО – формированием уполномоченным администратором предупреждающего сообщения перед установлением сеанса пользователя.

FMT_MTD.1 (11) – включен в связи с дополнительной возможностью ОО – установлением и модификацией уполномоченным администратором размера журнала аудита.

FMT_MTD.1 (12) – включен в связи с дополнительной возможностью ОО – управлением пороговым значением продолжительности бездействия уполномоченного пользователя в течение интерактивного сеанса уполномоченным пользователем.

FRU_PRS.1 – включен в связи с дополнительной возможностью ОО – установлением приоритетов субъектам для обеспечения доступа к процессорному ресурсу.

FRU_RSA.1 – включен в связи с дополнительной возможностью ОО – установлением максимальных квот на использование пользователями томов NTFS.

FTA_SSL.2 – включен в связи с дополнительной возможностью ОО – осуществлением пользователем блокирования и разблокирования собственного сеанса.

FTA_TAB.1 – включен в связи с дополнительной возможностью ОО – отображением перед открытием сеанса пользователя предупреждающего сообщения.

Добавленные в настоящее ЗБ функциональные требования не противоречат функциональным требованиям ПЗ.

8 Обоснование

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

8.1 Логическое обоснование целей безопасности

8.1.1 Логическое 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 для ОО на угрозы и политику безопасности организации.

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

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Audit_Protection	O.Residual_Information	O.Manage	O.Enforcement	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.Sec	O.Filtration
P.Sec												X	
P.Filtration													X

O.Authorization

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

O.Discretionary_Access

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

O.Auditing

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

O.Audit_Protection

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

O.Residual_Information

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

O.Manage

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

O.Enforcement

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

O.Protect

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

O.Legal_Warning

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

O.Limit_Authorization

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

O.Sec

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

O.Filtration

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.Filtration,** так как обеспечивает фильтрацию входящих в ОО информационных потоков.

8.1.2 Логическое обоснование целей безопасности для среды

В таблице 8.2 приведено отображение целей безопасности для среды на предположения безопасности.

Таблица 8.2 – Отображение целей безопасности для среды на предположения безопасности.

	OE.Install	OE.Physical	OE.Creden	OE.Trusted_Load	OE.Disable_Debugger
A.Connect		X			
A.Peer	X				
A.Coop			X		
A.Manage	X				
A.No_Evil_Adm	X				
A.Locate		X			
A.Protect		X			
A.Trusted_Load				X	
A.Disable_Debugger					X

OE.Install

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

OE.Physical

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

OE.Creden

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

OE.Trusted_Load

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Trusted_Load,** так как обеспечивает выполнение загрузки ОО в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование инструментальных средств, позволяющих осуществить доступ к защищаемым ресурсам ОО в обход механизмов защиты.

OE.Disable_Debugger

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Disable_Debugger,** так как для предотвращения несанкционированного доступа к системным компонентам в ОО исключена возможность запуска встроенных программ отладки.

8.2 Логическое обоснование требований безопасности

8.2.1 Логическое обоснование функциональных требований безопасности

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

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

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Audit_Protection	O.Residual_Information	O.Manage	O.Enforcement	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.Sec	O.Filtration
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												
FIA_ATD.1	X	X									X		
FIA_SOS.1	X												
FIA_UAU.2	X												
FIA_UAU.7	X												
FIA_UID.2	X												
FIA_USB.1		X	X										
FMT_MOF.1 (1)						X							
FMT_MOF.1 (2)	X					X							
FMT_MSA.1 (1)		X				X							

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Audit_Protection	O.Residual_Information	O.Manage	O.Enforcement	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.Sec	O.Filtration
FMT_MSA.1 (2)						X							X
FMT_MSA.1 (3)						X							X
FMT_MSA.3 (1)		X				X							
FMT_MSA.3 (2)						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.1 (9)						X							
FMT_MTD.1 (10)						X				X			
FMT_MTD.1 (11)			X			X							
FMT_MTD.1 (12)	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							
FPT_AMT.1								X					
FPT_ITC.1												X	
FPT_RVM.1							X						
FPT_SEP.1							X	X					
FPT_STM.1			X										
FPT_TST.1								X					
FRU_PRS.1	X												
FRU_RSA.2	X												
FTA_SSL.1	X												
FTA_SSL.2	X												
FTA_TAB.1										X			
FTA_TSE.1	X												

	O.Authorization	O.Discretionary_Access	O.Auditing	O.Audit_Protection	O.Residual_Information	O.Manage	O.Enforcement	O.Protect	O.Trusted_Path	O.Legal_Warning	O.Limit_Authorization	O.Sec	O.Filtration
FTP_TRP.1									X				

FAU_GEN.1 Генерация данных аудита

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

FAU_GEN.2 Ассоциация идентификатора пользователя

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

FAU_SAR.1 Просмотр аудита

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

FAU_SAR.2 Ограниченный просмотр аудита

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

FAU_SAR.3 Выборочный просмотр аудита

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

FAU_SEL.1 Избирательный аудит

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

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает защиту журнала аудита от несанкционированного изменения. При этом доступ к журналу аудита разрешен только администратору ОО. 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 администратору ОО в случае превышения журналом аудита определенного размера. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FAU_STG.4 Предотвращение потери данных аудита

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

FDP_ACC.1 Ограниченное управление доступом

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

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Выполнение требований данного компонента обеспечивает осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, 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.Filtration** 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.Filtration** и способствует ее достижению.

FDP_RIP.2 Полная защита остаточной информации

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

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает ограничение попыток пройти процедуру аутентификации для лиц, не являющихся санкционированными

пользователями. При достижении или превышении определенного администратором ОО числа неуспешных попыток аутентификации некоторого лица, данное лицо лишается возможности предпринимать дальнейшие попытки пройти процедуру аутентификации. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержку для каждого пользователя списка атрибутов безопасности, в том числе и идентификатора пользователя. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Discretionary_Access** 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 целью **O.Authorization** и способствует ее 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 пользователя обратная связь предоставляется в скрытом виде. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

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

FIA_USB.1 Связывание пользователь-субъект

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

FMT_MOF.1 (1) Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает модификацию и определения режимов выполнения, отключения и подключения ряда функций (таких, например, как аудит, управление квотированием) только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.Manage** и способствует ее достижению.

FMT_MOF.1 (2) Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает управление функцией блокирования и разблокирования сеанса пользователя только администратору ОО и уполномоченному пользователю ОО. Рассматриваемый компонент сопоставлен с целями **O.Authorization** и **O.Manage** и способствует их достижению.

FMT_MSA.1 (1) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает ограничение возможности модификации атрибутов управления доступом объектов только определенным, согласно политике дискреционного управления доступа, субъектам.

Рассматриваемый компонент сопоставлен с целями **O.Discretionary_Access, O.Manage** и способствует их достижению.

FMT_MSA.3 (1) Инициализация статических атрибутов

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

FMT_MSA.1 (2) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает ограничение возможности модификации атрибутов безопасности, используемых в политике фильтрации информации, только администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Manage** и **O.Filtration** и способствует их достижению.

FMT_MSA.1 (3) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает ограничение возможности модификации правил, используемых в политике фильтрации информации, только администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Manage** и **O.Filtration** и способствует их достижению.

FMT_MSA.3 (2) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, используемых в политики фильтрации информации, и возможность для администратора ОО определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **O.Manage** и **O.Filtration** и способствует их достижению.

FMT_MTD.1 (1) Управление данными ФБО

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

FMT_MTD.1 (2) Управление данными ФБО

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

FMT_MTD.1 (3) Управление данными ФБО

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

FMT_MTD.1 (5) Управление данными ФБО

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

FMT_MTD.1 (6) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность модификации продолжительности блокировки учетной записи пользователя после

превышения порога неуспешных попыток аутентификации только администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Authorization, O.Manage** и способствует их достижению.

FMT_MTD.1 (7) Управление данными ФБО

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

FMT_MTD.1 (8) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность модификации представления времени ФБО только администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Auditing, O.Manage** и способствует их достижению.

FMT_MTD.1 (9) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность модификации установок квотирования на томах NTFS только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.Manage** и способствует ее достижению.

FMT_MTD.1 (10) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность модификации предупреждающего сообщения перед установлением сеанса пользователя только администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.Manage, O.Legal_Warning** и способствует их достижению.

FMT_MTD.1 (11) Управление данными ФБО

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

FMT_MTD.1 (12) Управление данными ФБО

Выполнение требований данного компонента ограничивает возможность изменения значений по умолчанию, модификации, удаления, очистки порогового значения продолжительности бездействия уполномоченного пользователя в течение интерактивного сеанса только уполномоченным пользователям ОО. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FMT_MTD.2 Управление данными ФБО

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

FMT_REV.1 (1) Отмена

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

FMT_REV.1 (2) Отмена

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

FMT_SAE.1 Ограниченная по времени авторизация

Выполнение требований данного компонента обеспечивает ограничение на возможность назначать срок действия для аутентификационных данных только администратору ОО. 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 определенной роли. Рассматриваемый компонент сопоставлен с целями **O.Manage, O.Limit_Authorization** и способствует их достижению.

FMT_SMR.3 Принятие ролей

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

FPT_AMT.1 Тестирование абстрактной машины

Данный компонент включен в ЗБ, для того, чтобы учесть зависимости выполнения требований компонента FPT_TST.1**.** Выполнение требований данного компонента обеспечивает тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной, при первоначальном запуске, периодически и по запросу уполномоченного пользователя ОО. Рассматриваемый компонент сопоставлен с целью **O.Protect** и способствует ее достижению.

FPT_ITC.1 Конфиденциальность экспортируемых данных ФБО при передаче

Выполнение требований данного компонента обеспечивает возможность защиты данных ФБО при передаче удаленным доверенным системам ИТ (в т.ч. возможность защиты аутентификационной информации при передаче на контроллер 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 администратору ОО средство верификации целостности кода ФБО и данных. 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.2 Минимальные и максимальные квоты

Выполнение требований данного компонента обеспечивает реализацию максимальных квот на томах NTFS и минимальное количество процессорного ресурса, которое будет доступно для субъектов. 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 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. Определяются действия, необходимые для разблокирования. Рассматриваемый компонент сопоставлен с целью **O.Authorization** и способствует ее достижению.

FTA_TAB.1 Предупреждения по умолчанию перед предоставлением 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.

FTA_TSE.1 Открытие сеанса с ОО

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

FTP_TRP.1 Доверенный маршрут

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

8.2.2 Логическое обоснование требований доверия

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

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

8.2.3 Логическое 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.

Функциональный компонент	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 (2)
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3 (1)
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, FMT_MSA.3 (2)
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 (1)	FMT_SMR.1	FMT_SMR.1
FMT_MOF.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1 (1)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.1 (2)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.1 (3)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.3 (1)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (1), FMT_SMR.1
FMT_MSA.3 (2)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (2), FMT_MSA.1 (3), 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

Функциональный компонент	Зависимости по ОК	Удовлетворение зависимостей
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.1 (9)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (10)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (11)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1 (12)	FMT_SMR.1	FMT_SMR.1
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	FMT_MTD.1 (3), 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, FPT_STM.1	FMT_SMR.1, FPT_STM.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_SMR.3	FMT_SMR.1	FMT_SMR.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

Усиление ОУД1 компонентом AVA_SOF.1 (Оценка стойкости функции безопасности) требует включения в ЗБ для удовлетворения зависимостей компонента требований доверия к безопасности – ADV_HLD.1 (Описательный проект верхнего уровня). Это включение вызвано тем, что оценщику могла бы потребоваться информация из проекта верхнего уровня для анализа того, как работают несколько разных механизмов для обеспечения функции безопасности «Аутентификация». Минимальный уровень такой информации предоставляется через зависимость ADV_HLD. Но, так как функция безопасности «Аутентификация» в рассматриваемом ОО обеспечивается одним механизмом – «механизмом пароля», а информация об этом механизме подробно изложена в ЗБ, функциональной спецификации и руководствах, то зависимостью ADV_HLD.1 (Описательный проект верхнего уровня) можно пренебречь.

Таким образом, все зависимости включенных в ЗБ требований были удовлетворены.

8.3 Логическое обоснование краткой спецификации ОО

Таблица 8.5 – Отображение функциональных требований безопасности на функции безопасности

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Использование ресурсов	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.2		X					
FIA_AFL.1			X				
FIA_ATD.1			X				
FIA_SOS.1			X				
FIA_UAU.2			X				
FIA_UAU.7			X				
FIA_UID.2			X				
FIA_USB.1			X				
FMT_MOF.1 (1)				X			
FMT_MOF.1 (2)				X			
FMT_MSA.1 (1)		X					
FMT_MSA.1 (2)		X					

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Использование ресурсов	Блокирование сеанса
FMT_MSA.1 (3)		X					
FMT_MSA.3 (1)		X					
FMT_MSA.3 (2)		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.1 (9)				X			
FMT_MTD.1 (10)			X				
FMT_MTD.1 (11)	X						
FMT_MTD.1 (12)							X
FMT_MTD.2				X			
FMT_REV.1 (1)				X			
FMT_REV.1 (2)		X					
FMT_SAE.1				X			
FMT_SMR.1				X			
FMT_SMR.3			X				
FPT_AMT.1					X		
FPT_ITC.1					X		
FPT_RVM.1					X		
FPT_SEP.1					X		
FPT_STM.1					X		
FPT_TST.1					X		
FRU_PRS.1						X	
FRU_RSA.2						X	

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Использование ресурсов	Блокирование сеанса
FTA_SSL.1							X
FTA_SSL.2							X
FTA_TAB.1			X				
FTA_TSE.1			X				
FTP_TRP.1			X				

Таблица 8.6 – Отображение требований доверия на меры безопасности

	Управление конфигурацией	Руководства	Проектная документация	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 Логическое обоснование требований к стойкости функций безопасности

Термин «стойкость функции» определен в части 1 ОК как характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного режима при прямой атаке на лежащие в ее основе механизмы безопасности. В части 1 ОК определено три уровня стойкости функции: базовая СФБ, средняя СФБ и высокая СФБ. В настоящем 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. Логическое обоснование выбора средней СФБ определяется соответствием настоящего ЗБ ПЗ «Операционные системы. Клиентские операционные системы. Профиль защиты. Версия 1.0, 2003». Выбор средней СФБ в качестве минимального уровня стойкости функций безопасности является достаточным для определения допустимости использования ОО при обработке конфиденциальной информации.