| | |
|---|---|
| **СОГЛАСОВАНО** | **УТВЕРЖДАЮ** |
| Начальник 2 управления | Генеральный директор |
| ФСТЭК России | ЗАО «АЛТЭКС-СОФТ» |
| В. Селин | В. Сердюк |
| «  »_____ 2009 года | «  »_____ 2009 года |

# Операционная система Microsoft Windows Server 2008 Enterprise Edition

# Задание по безопасности

# MS.Win_Srv2008_EE.ЗБ

Версия 1.0

2009

СОДЕРЖАНИЕ

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| | |
|---|---|
| БД | – база данных |
| ЗБ | – задание по безопасности |
| ИТ | – информационная технология |
| МЭ | – межсетевой экран |
| МВМ | – монитор виртуальных машин |
| НСД | – несанкционированный доступ |
| ОГП | – объекты групповой политики |
| ОДФ | – область действия функций безопасности объекта оценки |
| ОК | – Общие критерии |
| ОО | – объект оценки |
| ОП | – организационное подразделение |
| ОС | – операционная система |
| ОУД | – оценочный уровень доверия |
| ПБО | – политика безопасности объекта оценки |
| ПЗ | – профиль защиты |
| ПФБ | – политика функции безопасности |
| СФБ | – стойкость функции безопасности |
| УК | – управление конфигурацией |
| ФБО | – функции безопасности объекта оценки |
| ФТБ | – функциональные требования безопасности |
| ACE | – Access Control Entry |
| ACL | – Access Control Lists |
| AD DS | – Active Directory Domain Services |
| AD LDS | – Active Directory Lightweight Directory Services |
| AD RMS | – Active Directory Rights Management Services |
| AD CS | – Active Directory Certificate Services |
| AD FS | – Active Directory Federation Services |
| AS | – Authentication Service |
| ASR | – Automated System Recovery |

DACL – Discretional Access Control List
DDE – Dynamic Data Exchange
DFS – Distribution File System
DNS – Domain Name System
GINA – Graphical Identification and Authentication
GPC – Group Policy Container
GPT – Group Policy Template
GUID – Globally Unique Identifier
IP – Internet Protocol
IPC – Interprocess Communication
KDC – Key Distribution Center
LPC – Local Procedure Call
LSA – Local Security Authority
LSASS – Local Security Authority Subsystem Service
LSS – Local Security Settings
LUID – Locally Unique Identifier
MMC – Microsoft Management Console
MMS – Microsoft Metadirectory Service
NAP – Network Access Protection
NAT – Network Address Translation
NDES – Network Device Enrollment Service
NLB – Network Load Balancing
NTFS – New Technology File System
ODBC – Open Database Connectivity
PDC – Primary Domain Controller
RID – Relative Identifiers
RID – Relative ID Manager
PXE – Pre-boot Execution Environment
SACL – System Access Control List
SAM – Security Account Manager
SAN – Storage Area Network

| | |
|---|---|
| SAS | – Secure Attention Sequence |
| SID | – Security Identifier |
| SNMP | – Simple Network Management Protocol |
| SNTP | – Simple Network Time Protocol |
| SQOS | – Security Quality of Service |
| SRM | – Security Reference Monitor |
| SCDPM | – System Center Data Protection Manager |
| SCVMM | – System Center Virtual Machine Manager |
| SSL | – Security Sockets Layer |
| SSO | – Single Sing-On |
| TGS | – Ticket Granting Service |
| TGT | – Ticket-Granting Ticket |
| UPnP | – Universal Plug and Play |
| VDS | – Virtual Disk Service |
| VSC | – Virtual Service Consumer |
| VSP | – Virtual Service Provider |
| WBEM | – Web-Based Enterprise Management |
| WEP | – Wired Equivalent Privacy |
| WFP | – Windows File Protection |
| WMI | – Windows Management Instrumentation |
| WSC | – Windows security center |
| WSUS | – Windows Server Update Services |
| UDDIS | – Universal Description, Discovery, and Integration Services |

# 1 Введение ЗБ

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

## 1.1 Идентификация ЗБ

| | |
|---|---|
| ***Название ЗБ:*** | Операционная система Microsoft Windows Server 2008 Enterprise Edition. Задание по безопасности. |
| ***Версия ЗБ:*** | Версия 1.0. |
| ***Обозначение ЗБ:*** | MS.Win_Srv2008_EE.ЗБ. |
| ***Идентификация ОО:*** | Операционная система Microsoft Windows Server 2008 Enterprise Edition. |
| ***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.<br>Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, Гостехкомиссия России, 2002.<br>Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности |

информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002.
Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.

***Ключевые слова:*** Операционная система, средство защиты информации, дискреционное управление доступом, задание по безопасности, ОУД1, Microsoft.

## 1.2 Аннотация ЗБ

Настоящее ЗБ определяет требования безопасности для операционной системы Microsoft Windows Server 2008 Enterprise Edition (далее – Server 2008).

Server 2008 – это серверная операционная система, предназначенная для организаций, которые ориентированы на серверные системы, требующие чрезвычайно масштабных возможностей по обработке и хранению данных, а также кластеризации или федеративных служб Active Directory (Active Directory Federation Services).

Server 2008 – это операционная система, обеспечивающая надежную, гибкую и масштабируемую платформу для автоматизации различных бизнес-задач. Новые средства виртуализации, поддержка современных веб-технологий и расширения в области безопасности помогают сократить время, требующееся на развертывание и сопровождение приложений, снизить затраты на обслуживание. Новые и расширенные компоненты операционной системы, такие как Internet Information Services 7.0 (IIS7), Windows Server Manager и Windows PowerShell, позволяют упростить задачи управления серверами и облегчить конфигурацию и сопровождение. Новые технологии безопасности Network Access Protection и Read-Only Domain Controller делают операционную систему более защищенной и позволяют использовать ее в качестве платформы для выполнения различных бизнес-задач.

## 1.3 Соответствие ОК

Объект оценки и ЗБ согласованы со следующими спецификациями:

– ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005» (**соответствие ПЗ** – ОО соответствует всем частям данного ПЗ);
– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002 (**расширение части 2 ОК** – ОО соответствует функциональным требованиям, основанным на функциональных компонентах из части 2 ОК, а также включающим функциональные компоненты, не содержащиеся в части 2 ОК);
– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002 (**усиление части 3 ОК** – требования доверия представлены в виде ОУД1 и, кроме того, включают компонент AVA_SOF.1 из части 3 ОК).

## 1.4 Соглашения

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

Операция **«уточнение»** используется для добавления к требованию некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей его удовлетворения. Результат операции **«уточнение»** в настоящем ЗБ обозначается **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 операции «итерация» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

В настоящее ЗБ включен компонент функциональных требований безопасности, сформулированный в явном виде. Краткая форма имени функционального компонента, сформулированного в явном виде, содержит текст (EXT).

## 1.5 Термины и определения

В настоящем ЗБ применяются следующие термины с соответствующими определениями.

**Активы** – информация или ресурсы ОО, подлежащие защите контрмерами ОО.

**Аутентификационные данные** – информация, используемая для верификации предъявленного идентификатора.

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

**Достоверность** – характеристика безопасности активов, обеспечивающая соответствие предусмотренным значениям.

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

**Задание по безопасности** – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО (в данном случае – ОС Microsoft Windows Server 2008 Enterprise Edition).

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

**Конфиденциальность** – характеристика защищенности информации ограниченного доступа от неправомочного раскрытия.

**Лес** – группа доменов в службе Active Directory.

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

**Объект оценки** – подлежащая оценке ОС Microsoft Windows Server 2008 Enterprise Edition с руководствами по эксплуатации.

**Подконтрольность** – характеристика безопасности активов, обеспечивающая 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.

**Администратор ОО** – уполномоченный пользователь, ответственный 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 (вычислительные возможности, физическая память, дисковое пространство).

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

**Субъект (субъект доступа)** – 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** – характеристика защищенности информации от модификации, подмены и уничтожения неправомочным способом.

## 1.6 Организация ЗБ

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

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

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

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

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

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

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

В Разделе 8 «Обоснование» демонстрируется, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает идентифицированные аспекты среды безопасности ИТ, а также что функции безопасности ИТ и меры доверия к безопасности соответствуют требованиям безопасности ОО.

# 2 Описание ОО

Объектом оценки является операционная система Microsoft Windows Server 2008 Enterprise Edition (32-бит и 64-бит версии) с установленным пакетом обновления Windows 6.0-KB950050-x64.msu, для включения роли Hyper-V.

## 2.1 Тип продукта ИТ

Операционная система Microsoft Windows Server 2008 Enterprise Edition – полнофункциональная серверная многозадачная и многопользовательская операционная система общего назначения.

Единое использование ряда технологий в области сетевой поддержки, хранения, безопасности и управления обеспечивает совместную работу Server 2008 с ОС Windows Vista.

Windows Server Virtualization (механизмы виртуализации) и System Center Virtual Machine Manager, используемые в Server 2008 позволяют снизить затраты, повысить эффективность использования аппаратных средств оптимизировать инфраструктуру и увеличить доступность серверов. Виртуализация в Server 2008 использует 64-разрядную платформу на основе гипервизора, что позволяет увеличить производительность, надежность и масштабируемость. Помимо этого виртуализация использует такие компоненты платформы Server 2008, как отказоустойчивые кластеры, для обеспечения высокой доступности и защиты доступа к сети – Network Access Protection.

Internet Information Services 7.0 (IIS7) – Интернет-платформа для приложений и служб. Эта модульная платформа имеет более простой интерфейс управления на основе задач и интегрированные средства управления состоянием веб-служб, обеспечивает строгий контроль над взаимодействием узлов и содержит ряд усовершенствований безопасности.

IIS7 и .NET Framework 3.0 формируют комплексную платформу для разработки приложений, которые связывают пользователей друг с другом и с данными, обеспечивая в результате наглядное представление, совместное использование и обработку информации

Server 2008 – наиболее защищенный из всех продуктов Windows Server. Повышенная безопасность операционной системы и новшества системы безопасности, включая систему защиты доступа к сети, контроллер домена только для чтения,

обеспечивают максимальный уровень защиты сети, данных и бизнеса. Server 2008 позволяет защитить серверы, сети, данные и учетные записи пользователей от сбоев и вторжений. Технология защиты доступа к сети позволяет изолировать компьютеры, которые не отвечают требованиям действующих политик безопасности, и обеспечивает для сети механизм ограничения доступа, устранения недостатков и непрерывной проверки соответствия. Федеративные службы управления правами поддерживают постоянную защиту конфиденциальных данных, помогают сократить риски, обеспечивают соблюдение регулятивных норм и формируют платформу для комплексной защиты информации. Контроллер домена только для чтения (RODC) позволяет развертывать службы Active Directory с ограниченной репликацией полной базы данных Active Directory для улучшения защиты на случай кражи или взлома сервера.

Server 2008 – самая гибкая и надежная операционная система семейства Windows Server. Благодаря новым технологиям, таким как установка основных компонентов сервера, PowerShell, инструментарий Windows Deployment Services, а также улучшенным сетевым технологиям и технологиям кластеризации, Server 2008 обеспечивает самую универсальную и надежную платформу Windows для всех имеющихся приложений и рабочей нагрузки.

Диспетчер серверов ускоряет установку и настройку серверов и упрощает текущее управление серверными ролями из единой консоли.

Windows PowerShell – новая оболочка с интерфейсом командной строки, поддерживающая более 130 командных средств (называемых командлетами) и встроенный язык программирования, позволяет администратору автоматизировать выполнение рутинных операций по управлению системами, особенно на нескольких серверах.

Вариант установки Windows Server Core (основные компоненты сервера) – новый вариант установки выбранных ролей, при котором развертываются только нужные компоненты и подсистемы без графического интерфейса пользователя, в результате чего создается сервер с высокой отказоустойчивостью, требующий меньше обслуживания и обновления.

## 2.2 Основные функциональные возможности операционной системы Microsoft Windows Server 2008 Enterprise Edition

В ОС Microsoft Windows Server 2008 Enterprise Edition реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность ИТ, надежность Server 2008, а также упрощающих администрирование и управление вычислительной средой Server 2008. В данном подразделе представлено краткое описание этих функциональных возможностей и средств ОС.

### 2.2.1 Основные функциональные возможности обеспечения безопасности

В Server 2008 включены средства, позволяющие защитить выбранные файлы, приложения и ресурсы. В число таких средств входят списки управления доступом ACL, 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

Server 2008 располагает широким набором шаблонов политик безопасности, которые могут применяться для управления конфигурацией безопасности компьютеров в конкретной вычислительной среде и параметрами безопасности, затрагивающими учетные записи пользователей. Применение групповой политики осуществляется с целью контроля использования пользователями программ, сетевых ресурсов и централизованного задания единых параметров безопасности управляемых ОС.

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

Интегрирование групповой политики со службой каталогов Active Directory позволяет обеспечить 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 обеспечивает 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 Server 2008, позволяет обеспечить безопасную среду для пользователей, ограничив их доступ к запрещенным программам и данным, системным параметрам Server 2008, исключить возможность 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.

#### 2.2.1.2 Политика ограниченного использования программ

С помощью политики ограниченного использования программ (software restriction policy) в Server 2008 реализуется изоляция подозрительного, потенциально опасного (недоверенного) кода, обеспечивается защита компьютера от различных вирусов, «троянских» программ, сетевых и почтовых «червей», а также других вредоносных программ.

В операционной системе Server 2008 для разрешения или запрещения исполнения программ определены уровни безопасности: «неограниченный» (unrestricted) или «не разрешено» (disallowed). Уровень безопасности «не разрешено» применяется для всех программ по умолчанию, однако уполномоченные администраторы могут определять дополнительные правила, разрешающие выполняться отдельным программам.

Политика ограниченного использования программ включает уровень безопасности, устанавливаемый по умолчанию («не разрешено»), и все дополнительно определяемые правила. Данная политика может быть применена ко всему домену, к отдельным компьютерам или пользователям. Она предоставляет разные способы идентификации программ, а также основанную на политике инфраструктуру, принудительно реализующую решения об исполнении той или иной программы.

Политика ограниченного использования программ позволяет:

- управлять возможностью исполнения программ на компьютерах;
- разрешить запуск на выполнение только определенных файлов;
- определять, кому предоставлено право добавлять производителей программ в список доверенных производителей (trusted publishers);

– задавать степень влияния политики ограниченного использования программ – на всех, либо только на некоторые категории пользователей компьютера;
– запрещать исполнение любых выбранных файлов на локальном компьютере.

#### 2.2.1.3 Группы безопасности

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

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

После установки в Server 2008 по умолчанию создаются встроенные группы, дающие право выполнять предопределенные системные задачи. Исходя из модели построения сети – модель рабочей группы (workgroup) или доменная модель (domain)– встроенные группы подразделяются на:

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

#### 2.2.1.4 Списки управления доступом

В Server 2008 доступ к активам системы разрешен только уполномоченным на это пользователям. Модель защиты Server 2008 включает компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа и аудит событий.

Каждый объект доступа, представленный в Server 2008, однозначно ассоциирован с дескриптором безопасности, главными компонентами которого являются: дискреционный список контроля доступа, который определяет права доступа к объекту и системный список контроля доступа, служащий для определения параметров аудита. 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

Операционная система Server 2008 располагает достаточным набором 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 безопасности и учетными записями пользователей, а также вход пользователей в систему и выход из нее. В частности, аудит позволяет вести мониторинг конкретных событий, например, неудачных попыток входа в систему. Просмотр журнала безопасности выполняется с помощью средства просмотра событий. Политика аудита позволяет определять, для каких категорий событий должен проводиться аудит.

#### 2.2.1.6 Принудительное применение учетной записи гостя

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

Действие данной политики не распространяется при использовании учетных записей домена, а также на интерактивный доступ, выполняемый в удаленном режиме с использованием таких служб, как Telnet или службы терминалов. Для всех компьютеров по умолчанию используется политика принудительного применения учетной записи гостя.

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

Если действует политика «принудительное назначение прав гостя при входе с локальной учетной записью» (force network logons using local accounts to authenticate as Guest), локальная учетная запись должна идентифицироваться как «гость». Эта политика определяет, следует ли обязательно идентифицировать пользователя, который устанавливает подключение из сети непосредственно к компьютеру, как гостя. Таким образом, ограничиваются разрешения, предоставляемые локальным пользователям, пытающимся получить доступ к активам данного компьютера. Если эта политика включена, всем локальным пользователям, пытающимся непосредственно подключиться к компьютеру, предоставляется уровень разрешений гостя, который, как правило, существенно ограничен.

#### 2.2.1.7 Ограничения на пустой пароль

В ОС Server 2008 реализована функция ограничения использования в учетных записях пустого и простого пароля. При первоначальном входе в ОС администратору предлагается сменить пароль. В случае ввода простого или пустого пароля, система выдает предупреждение и блокирует регистрацию. Необходимо повторить ввод пароля с длинной не менее 8 символов, с цифрами и как минимум одной строчной буквой. Учетная запись с таким паролем подлежит регистрации и доступ в ОС Server 2008 разрешается.

#### 2.2.1.8 Управление учетными данными

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

доступа к этому приложению сохраненные учетные данные будут использоваться повторно, их не потребуется вводить повторно.

#### 2.2.1.9 Хранение имен пользователей и паролей

Хранение имен пользователей и паролей осуществляется в безопасном перемещаемом хранилище. Доступ к учетным данным регулируется параметрами локальной безопасности LSS. Целевая информация, возвращаемая ресурсом, влияет на хранение учетных данных.

### 2.2.2 Основные функциональные возможности повышения надежности

Операционная система Server 2008 обеспечивает надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая описанные в п.п. 2.2.2.1-2.2.2.10 возможности по повышению надежности.

#### 2.2.2.1 Защита файлов Windows

Подсистема WFP обеспечивает защиту от перезаписи и удаления защищаемых системных файлов с расширением *.sys, *.dll, *.ocs, *.ttf, *.exe и некоторых файлов *.fon. Средства защиты файлов Windows работают в фоновом режиме и предотвращают возможность изменения или замещения системных файлов другими программами. Данный механизм позволяет исключить вероятность аварийного завершения работы системы или отказа приложений в случаях модификации, перемещения или удаления системных файлов, произошедших по неосторожности или в результате воздействия вирусов и других вредоносных программ.

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

В зависимости от параметров, заданных администратором при настройке компьютера, Server 2008 либо игнорирует драйверы устройств, не имеющие цифровой

подписи, либо предупреждает об обнаруженных драйверах без цифровой подписи (этот режим принимается по умолчанию), либо запрещает установку неподписанных драйверов.

#### 2.2.2.2 Мониторинг завершения работы

Операционная система Server 2008 содержит утилиту мониторинга завершения работы сервера (Shutdown Event Tracker), использующую механизм детального документирования причин отключения и перезапуска компьютера. Эти данные используются для анализа причин аварийного завершения работы компьютера и более полного анализа системной среды.

Кроме документирования причин завершения работы, утилита Shutdown Event Tracker также осуществляет «моментальный снимок» состояния системы перед отключением, определяет, какие системные ресурсы были перегружены или близки к перегрузке. Она также регистрирует ряд параметров всех процессов в системе, страничных файлов, дисков и общие сведения об использовании системных ресурсов.

#### 2.2.2.3 Верификация приложений

Приложения, исполняющиеся в среде ОС Server 2008, могут быть протестированы с использованием инструментального средства Windows Application Verifier, которое позволяет выявить дефекты структур управления памятью и проблемы совместимости данного приложения с операционной системой. Кроме того, использование данного инструмента позволяет выявить возможные проблемы безопасности, которые могут возникнуть при функционировании приложения, такие как запись информации в неверный раздел реестра или каталог файловой системы. Использование механизма верификации приложений не позволяет полностью исключить возможные проблемы безопасности или совместимости приложений, но предоставляет возможность избежать большинства из них.

#### 2.2.2.4 Архивация данных

В ОС Server 2008 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.

#### 2.2.2.5 Теневое копирование тома

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

#### 2.2.2.6 Служба виртуальных дисков

Служба виртуальных дисков VDS обеспечивает управление аппаратными и программными томами посредством использования единого унифицированного интерфейса управления дисками.

В ОС Server 2008 реализованы провайдеры VDS для базовых и динамических дисков. Возможности управления базовыми дисками позволяют обеспечить набор действий аналогичных возможностям управления динамическими дисками (например, увеличение размера тома «на лету»).

#### 2.2.2.7 Откат драйверов

Данная возможность способствует обеспечению устойчивости ОС Server 2008. При обновлении драйвера копия предыдущего пакета драйверов автоматически сохраняется в специальном подкаталоге системных файлов (для каждого архивируемого драйвера добавляется новое значение к ключам архивации, размещенным в соответствующем разделе реестра). Если новый драйвер будет работать неудовлетворительно, пользователь может восстановить предыдущую версию драйвера, перейдя в «Диспетчере устройств» на вкладку «Драйвер» (Driver) для соответствующего устройства и нажав кнопку «Откатить» (Roll Back Driver). Откат драйвера разрешается производить на один предшествующий уровень, поскольку только одна версия предыдущего драйвера может сохраняться при

выполнении обновления. Данная возможность доступна для всех классов устройств, за исключением принтеров.

#### 2.2.2.8 Восстановление системы

Функциональная возможность восстановления системы позволяет возвращать компьютер в то состояние, в котором он находился до возникновения проблемы. При этом не происходит потери личных файлов данных, которые могут содержать, например, документы, изображения или сообщения электронной почты. При использовании данной возможности осуществляется активный мониторинг изменений системных характеристик и некоторых файлов приложений, а также автоматическое создание легко идентифицируемых контрольных точек восстановления. В ОС Server 2008 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.

#### 2.2.2.9 Аварийное восстановление системы

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

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

#### 2.2.2.10 Консоль восстановления

Консоль восстановления позволяет запустить при возникновении программных сбоев окно командной строки, предоставляющее ограниченный набор административных команд, предназначенных для восстановления работоспособности операционной системы.

Консоль восстановления обеспечивает администратора ОС Server 2008 возможностями запуска и остановки служб ОС Server 2008, форматирования диска, считывания и записи данных, а также выполнения ряда других задач администрирования.

### 2.2.3 Основные средства администрирования, управления и поддержки

Средства администрирования, управления и поддержки обеспечивают полномасштабное и гибкое управление ОС Server 2008. Краткое описание основных из них представлено в п.п. 2.2.3.1-2.2.3.7.

#### 2.2.3.1 Служба каталогов Active Directory

Служба каталогов Active Directory является одним из центральных компонентов ОС Server 2008 и предоставляет средства управления объектами и взаимосвязями сетевой среды.

Служба каталогов Active Directory хранит данные об объектах в вычислительной сети и обеспечивает удобные средства для поиска и использования этих сведений. В качестве основы для логической, иерархической организации информации служба каталогов Active Directory использует структурированное хранилище данных, содержащее данные о таких объектах, как пользователи, группы безопасности и распространения, компьютеры, домены, организационные подразделения и правила политики безопасности.

Служба каталогов Active Directory позволяет пользователям вычислительной сети осуществлять доступ к защищаемым активам в рамках одного процесса подключения. Кроме того, эта служба обеспечивает администраторов интуитивным иерархическим представлением вычислительной сети и единым инструментом администрирования всех сетевых объектов.

Служба каталогов Active Directory поддерживает ряд безопасных протоколов Интернета и протоколов аутентификации пользователей при их доступе в системы, включая Kerberos v.5 rev.6, цифровые сертификаты X.509 v.3 и смарт-карты.

Служба каталогов Active Directory включает в себя:

- аудит (AD DS: Auditing):
  - доступ к службе каталогов (Directory Service Access);
  - доступ к службе изменений каталогов (Directory Service Changes);
  - доступ к службе репликации каталогов (Directory Service Replication);
  - доступ к службе детальной репликации каталогов (Detailed Directory Service Replication);
- разветвленные политики паролей (AD DS: Fine-Grained Password Policies) предоставляет следующие возможности:
  - политика паролей:
    - внедрение истории паролей (Enforce password history);
    - максимальный срок действия пароля (Maximum password age);
    - минимальный срок действия пароля (Minimum password age);
    - минимальная длина пароля (Minimum password length);
    - пароли должны соответствовать требованиям сложности (complexity requirements);
    - хранение паролей с использованием обратимого шифрования (reversible encryption);
  - политика блокировки (Lockout Policy):
    - длительность блокировки учетной записи (Account lockout duration);
    - порог блокировки учетной записи (Account lockout threshold);
    - восстановить блокировку учетной записи после (Reset account lockout after);
- контроллеры доменов с доступом только чтение (AD DS: Read-Only Domain Controllers (RDOC). RODC – это новый тип контроллера доменов для Server 2008. Благодаря функции RODC, организации могут с легкостью разворачивать контроллеры доменов в тех местах, где физически нельзя гарантировать безопасность. Основы RODC следующие:
  - контроллер домена, доступный только для чтения (Read-Only Domain Controller);
  - разделение административных ролей (Administrative Role Separation);

  - кэширование мандатов (Credential Caching);
  - служба доменных имен, доступная только для чтения (Read-Only DNS);
- службы рестарта AD (AD DS: Restartable Active Directory Domain Services). В Server 2008 службы Active Directory Domain Services теперь можно останавливать и перезапускать. Это означает, что вы можете остановить AD DS, чтобы выполнить определенные задания и обслуживание, что в предыдущих версиях Windows Server требовало перезагрузки в режиме Directory Services Restore Mode DSRM). Это отличная характеристика для прописывания сценариев и автоматизации этих заданий. Возможные режимы для AD DS:
  - AD DS − запущена;
  - AD DS − остановлена;
  - режим восстановления AD DS Restore Mode (DSRM);
- интеллектуальный инструмент анализа данных (AD DS: Database Mounting Tool). Эта функциональная возможность позволяет просматривать данные AD DS, хранящиеся в подключенных снимках состояния объектов, сделанных в различные моменты времени, и выбирать нужные для восстановления данные без необходимости перезагрузки сервера;
- усовершенствования интерфейса пользователя (AD DS: User Interface Improvements), предоставляют новые инсталляционные варианты контроллера домена, а также обеспечивают новые варианты управления параметрами AD DS, такими как RDOC.

#### 2.2.3.2 Диспетчер жизненного цикла идентификационных данных - ILM 2007

ILM 2007 (Identity Lifecycle Manager) обеспечивает администраторов единым интерфейсом для осуществления доступа к различным каталогам и конфигурирования способов, которыми между ними посредством метакаталога должна синхронизироваться и/или реплицироваться информация. ILM 2007 используется для управления идентификационными данными каталогов, т.е. для управления учетными записями пользователей путем синхронизации атрибутов наподобие идентификатора для входа в систему, имени, фамилии, номера телефона, наименования должности и названия отдела. Данный способ применения ILM 2007 называется управлением идентификацией. ILM

2007 также используется для инициализации и деинициализации учетных записей, т.е автоматического централизованного создания и удаления учетных записей пользователей, и управления группами.

#### 2.2.3.3 Использование дисковых квот

Механизм дисковых квот позволяет отслеживать и контролировать использование пользователями места на диске для томов NTFS. Администраторы могут настроить ОС Server 2008 таким образом, чтобы:

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

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

Механизм квотирования также распространяется на объекты службы каталогов Active Directory, предоставляя администратору ОС Server 2008 возможность управлять количеством объектов, владельцем которых может являться пользователь, группа или компьютер, в заданном разделе каталога Active Directory.

#### 2.2.3.4 Распределенная файловая система

Распределенная файловая система DFS предоставляет возможность создания дерева каталогов, включающего несколько файловых серверов и общие файлы для группы пользователей или организации. Такой способ представления ресурсов упрощает доступ пользователей к файлам, а также поиск файлов и папок, физически распределенных по

сети. Система DFS обеспечивает возможность предоставления пользователям файлов, находящихся на разных серверах, как если бы они находились в едином месте. Для доступа к таким файлам пользователям не потребуется указывать их действительное физическое расположение.

Операционная система Server 2008 обеспечивает поддержку нескольких корней DFS на одном сервере, что позволяет повысить надежность корней DFS путем применения кластерных архитектур. Функции администрирования DFS позволяют делегировать полномочия на управление различными частями пространства имен DFS, разным администраторам.

Общие объекты распределенной файловой систем могут быть опубликованы как объекты томов в каталоге Active Directory.

#### 2.2.3.5 Инструментарий управления Windows

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

WMI включает CIM-совместимую базу данных, в которой хранятся определения объектов, и диспетчер объектов CIM, в задачи которого входит занесение объектов в хранилище и управление ими, а также сбор данных от поставщиков WMI. Поставщики WMI играют роль посредников между WMI и компонентами операционной системы, приложениями и другими системами. Например, поставщик реестра получает данные из реестра, а поставщик SNMP предоставляет данные и события от устройств SNMP. Поставщики не только предоставляют данные, но и методы, с помощью которых можно управлять компонентами, свойства, которые могут быть изменены, и события, информирующие об изменениях, происходящих в компонентах.

WMI может использоваться средствами управления компьютерами, такими как Microsoft Systems Management Server. Кроме того, WMI применяется в других технологиях, таких как Microsoft Health Monitor и Microsoft Operations Manager, а также

сторонними изготовителями компьютерных систем управления. Можно также использовать WMI вместе с системами программирования (такими как Windows Script Host) как для получения сведений о конфигурации компьютерных систем, в том числе о серверных приложениях, так и для изменения конфигурации.

#### 2.2.3.6 Диспетчер сервера (Server Manager)

Диспетчер сервера − новый компонент операционной системы Server 2008. Он представляет собой единый интерфейс, через который ИТ-администратор может выполнять все действия по установке, настройке серверных ролей и компонентов Server 2008 и управлению ими с помощью новой консоли управления (Server Manager console). Диспетчер сервера объединяет в себе функции ряда компонентов Microsoft Windows Server 2003, таких как «Управление сервером», «Мастер настройки сервера» и «Установка и удаление программ».

С помощью диспетчера сервера можно настраивать на компьютере разные функции и компоненты. Роль сервера в Server 2008 описывает основное назначение сервера. Администратор может выделить под определенную роль весь сервер или установить несколько ролей на одном и том же компьютере.

Server Manager console расширяет возможности консоли управления Microsoft Management Console.

#### 2.2.3.7 Консоль управления MMC

Консоль управления MMC – средство для создания, сохранения и открытия средств администрирования (называемых оснастками MMC), с помощью которых осуществляется управление оборудованием, программными и сетевыми компонентами ОС Server 2008.

MMC не выполняет административные функции, но в ней размещаются инструменты, выполняющие эти функции. Основным типом инструментов, которые можно добавить в консоль, является оснастка. Другими добавляемыми элементами являются элементы управления ActiveX, ссылки на веб-страницы, папки, виды панели задач и задачи. Все функции управления в ОС Server 2008 доступны через оснастки консоли управления MMC.

### 2.2.3.8 Установка ядра сервера (Server Core installation)

В Server 2008 администратор имеет возможность установки ОС в минимальной конфигурации в режиме ограничения ролей сервера, что повышает безопасность системы, но ограничивает возможности функционала.

Server Core installations обеспечивает установку среды для выполнения следующих ролей:

- Active Directory Domain Services;
- Active Directory Lightweight Directory Services;
- DHCP Server;
- DNS Server;
- File Services;
- Print Server;
- Streaming Media Services.

### 2.2.3.9 Средства администрирования

В составе Server 2008 интегрированы следующие средства администрирования:

- **Служба терминалов** − предназначена для просмотра и отслеживания сведений о пользователях, сеансах и процессах на серверах терминалов, работающих под управлением Server 2008. Можно также выполнять некоторые задачи администрирования, например отключать пользователей от их сеансов служб терминалов или завершать эти сеансы;
- **Инициатор iSCSI** − это способ соединения устройств хранения данных через сеть с использованием протокола TCP/IP. Он может быть использован в локальной сети (LAN) глобальной сети (WAN) или Интернет;
- **Локальная политика безопасности** – это оснастка консоли управления (MMC), которая обеспечивает единый интерфейс управления всеми параметрами объектов локальной групповой политики (политика учётных записей, политики ограниченного доступа, Брандмауэра Windows, политик открытого ключа и пр.);

- **Обозреватель хранилищ** − проводник хранилищ предназначен для просмотра коммутирующих матриц Fibre Channel и iSCSI, доступных в сети хранения данных (SAN), и управления ими;
- **Система архивации данных Windows Server** − резервное копирование Windows Server - это инструмент Server 2008, предоставляющий набор мастеров и других средств выполнения основных задач резервного копирования и восстановления для сервера, на котором он установлен. Данная функция была переработана с добавлением новой технологии. Предыдущий инструмент резервного копирования (Ntbackup.exe), который был доступен в более ранних версиях Windows, был удален;
- **Средство диагностики памяти** − встроенное средство диагностики виртуальной памяти на предмет возникновения ошибок;
- **Брандмауэр Windows в режиме повышенной безопасности** − брандмауэр Windows в режиме повышенной безопасности объединяет брандмауэр узла и средства IPsec. В отличие от брандмауэра сетевого периметра, брандмауэр Windows в режиме повышенной безопасности работает на каждом компьютере под управлением данной версии Windows и обеспечивает локальную защиту от сетевых атак, проникающих в демилитаризованную зону или исходящих из внутренней сети организации. Он также обеспечивает безопасность соединения между компьютерами, что позволяет требовать проверки подлинности и защиты данных при обмене данными;
- **Управление компьютером** – используется для управления локальными или удаленными компьютерами. Оснастка «Управление компьютером» объединяет несколько средств администрирования ОС Server 2008 в одно дерево консоли, что обеспечивает легкий доступ к свойствам администрирования конкретного компьютера;
- **Источники данных (ODBC)** – ODBC (Open Database Connectivity) – программный интерфейс, с помощью которого программы получают доступ к данным в системах управления базами данных, использующих язык SQL как стандарт доступа к данным;

- **Мастер настройки безопасности** − мастер, позволяющий создать политику безопасности, которую можно применить для любого сервера в сети, эта политика настраивает службы и сетевую безопасность на основе исполняемых сервером ролей, а так же аудит и параметры реестра;
- **Планировщик заданий** − это оснастка MMC, позволяющая назначать автоматически выполняемые задания, запуск которых производится в определенное время или при возникновении определенных событий. Планировщик заданий содержит библиотеку всех назначенных заданий, обеспечивая возможность быстрого просмотра и удобного управления заданиями;
- **Службы** − оснастку «Службы» консоли управления (MMC) можно использовать для управления службами, которые запущены на локальном или удаленных компьютерах, чтобы, например, запустить или остановить службу;
- **Диспетчер сервера** − Server 2008 упрощает задачи управления и защиты нескольких ролей сервера в организации благодаря консоли Диспетчер сервера. Диспетчер сервера в Server 2008 представляет собой единое средство для управления сведениями об удостоверении сервера и системе, отображения состояния сервера, выявления проблем с конфигурацией роли сервера и управления всеми установленными на нем ролями;
- **Конфигурация системы** − программа настройки системы является дополнительным средством для выявления проблем, которые могут помешать запуску системы в обычном режиме, так же позволяет выбирать программы автозагрузки, запускаемые при запуске службы, режим загрузки системы и пр.;
- **Монитор производительности и стабильности** − Монитор производительности и стабильности Microsoft Windows можно использовать для анализа влияния работы программ на производительность компьютера как в реальном времени, так и посредством сбора данных журнала для последующей обработки. Монитор производительности и стабильности Windows использует счетчики производительности, данные трассировки событий и сведения о конфигурации, которые можно объединять в группы сборщиков данных;

- **Просмотр событий** − программа «Просмотр событий» представляет собой оснастку консоли управления MMC и предназначена для просмотра и управления журналами событий. Это незаменимый инструмент для наблюдения за работоспособностью системы и устранения возникших неполадок. С помощью программы «Просмотр событий» можно:
  - просматривать события из нескольких журналов;
  - сохранять удобные фильтры событий в виде настраиваемых представлений для дальнейшего использования;
  - назначать выполнение задачи в ответ на возникновение какого-либо события;
  - создавать и управлять подписками на события.
- **Службы компонентов** − с помощью оснастки «Службы компонентов» в MMC можно настраивать компоненты COM, приложения COM+ и координатора распределенных транзакций DTC, а также администрировать их. Оснастка «Службы компонентов» предназначена как для системных администраторов, так и для разработчиков приложений. Например, администраторы могут управлять компонентами, а разработчики могут настраивать требуемое поведение компонента и приложения, например участие в транзакциях и организации пула объектов;
- **Управление общими ресурсами и хранилищами** − оснастка «Управление общими ресурсами и хранилищами» − это основное средство управления общими ресурсами, такими как папки и тома, а также ресурсами хранилища.

#### 2.2.3.10 Виртуализация

Встроенные в Server 2008 технологии виртуализации позволяют снизить затраты, повысить эффективность использования аппаратных средств, оптимизировать инфраструктуру и увеличить доступность серверов. Виртуализация в Server 2008 использует 64-разрядную платформу на основе гипервизора (Hyper-V), что позволяет увеличить производительность, надежность и масштабируемость.

Технология Hyper-V − основа платформы виртуализации для серверов на базе процессоров с архитектурой x64. В Server 2008 технология Hyper-V может быть

развернута как в полной установке, так и в режиме Server Core. Это позволяет в полной мере реализовать все преимущества «тонкой», экономичной и управляемой платформы виртуализации.

Hyper-V является встроенным компонентом 64-разрядных версий Server 2008, в 32-разрядных версиях данная технология не доступна.

**Архитектура**

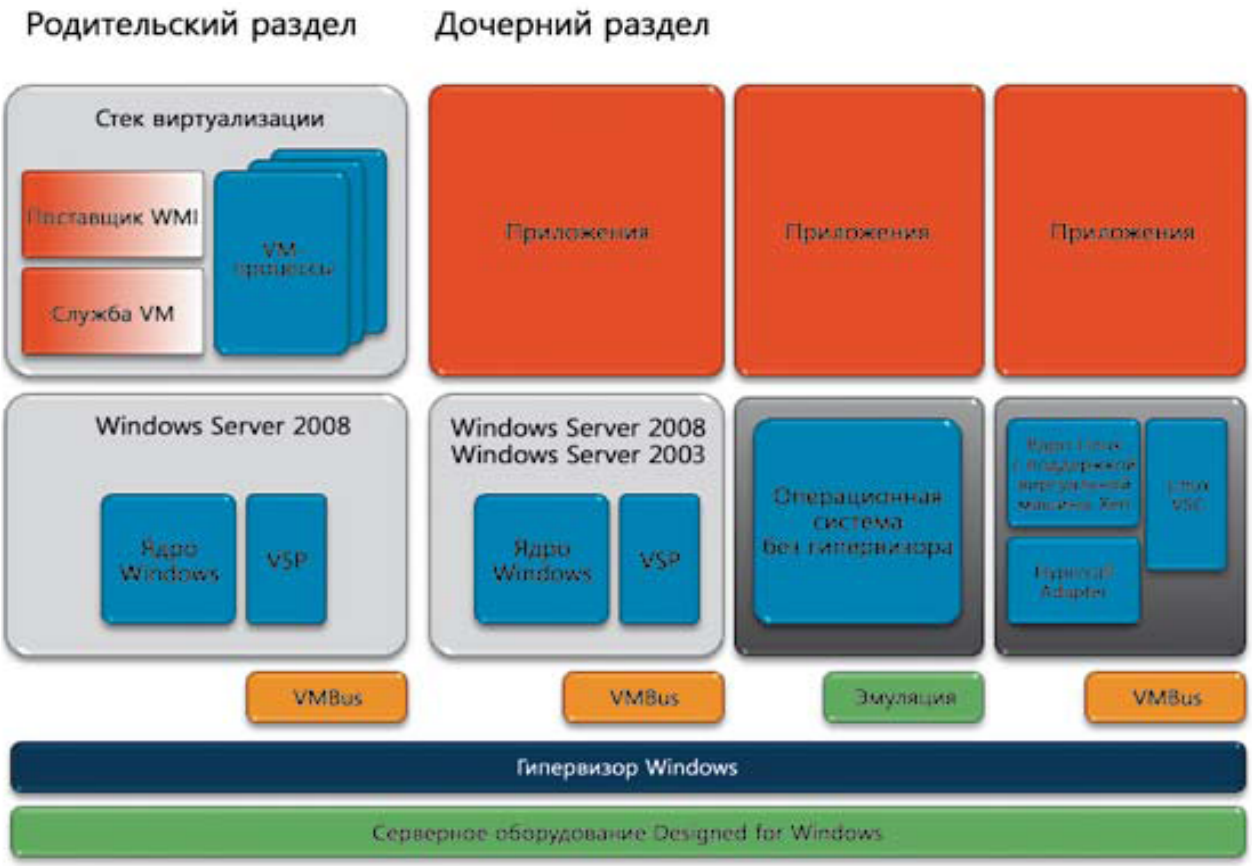
Hyper-V построен по принципу гипервизора с микроядром. Архитектура гипервизора предполагает, что МВМ устанавливается прямо поверх аппаратного обеспечения, в отличие от случая, где МВМ работает в среде хостовой операционной системы. Такой подход к построению МВМ позволяет достичь более высокой скорости работы, так как исключает накладные расходы, связанные с работой хостовой ОС. Установка Hyper-V производится включением соответствующей роли (Hyper-V) в консоли управления Server Manager Server 2008 или специальными командами в режиме Server Core. После активации данной опции и перезагрузки сервера в стеке программного обеспечения сервера появляется прослойка гипервизора, которая позволяет создавать и управлять логическими разделами сервера − виртуальными машинами.

Специальным разделом, существующим на сервере сразу после активации гипервизора, является так называемый родительский раздел. Этот раздел получает прямой доступ к оборудованию, такому как жесткий диск, сетевой адаптер и т.д. и отвечает за их совместное использование в виртуальных машинах. Гостевые виртуальные машины работают в изолированных от аппаратного обеспечения дочерних разделах.

Гипервизор Hyper-V является достаточно простым и содержит лишь базовую функциональность, во многом полагаясь на аппаратную виртуализацию. Основная логика по планированию распределения ресурсов между разделами, а также все программные компоненты, ответственные за администрирование системы виртуализации вынесены в родительский раздел. Поэтому архитектура гипервизора Hyper-V называется микроядерной. Использование микроядра обеспечивает ряд серьезных преимуществ:

– Hyper-V Windows не содержит кода (например, драйверов), разработанного другими производителями. Благодаря этому минимизируется потенциальная площадь атаки, как для гипервизора, так и для виртуальных машин;

– Hyper-V разработан с учетом аппаратных средств виртуализации, интегрированных в серверные платформы на базе процессоров Intel и AMD, позволяющих значительно повысить скорость работы при использовании виртуальных машин;
– Интеграция с операционной системой Server 2008 обеспечивает высокую надежность и масштабируемость системы виртуализации. Вместе с включенными в Server 2008 службами отказоустойчивой кластеризации быстрая миграция (автоматическое перемещение виртуальных машин при запланированном или незапланированном сбое в работе хоста и их запуск на другом хосте) позволяет поддерживать высокую степень доступности без дополнительных затрат. Кроме того, подобная интеграция позволяет обеспечить поддержку на сервере всего спектра оборудования, совместимого с Server 2008.



Архитектура разделения устройств ввода-вывода построена на системе синтетических устройств. В родительский раздел входят провайдеры служб виртуализации VSP, обменивающиеся информацией через VM-шину в памяти (точка-точка) для обслуживания запросов дочерних разделов при доступе к драйверам синтетических устройств. Соответственно, дочерние разделы включают в себя клиентов служб виртуализации VSC в виде драйверов синтетических устройств. Последние пересылают запросы для синтетического оборудования на VSP через VM-шину. Гостевые операционные системы, не имеющие интегрированных компонентов для Hyper-V, должны обходиться без VM-шины и, следовательно, используют эмулируемые драйверы оборудования. Для гостевых операционных систем эти процессы осуществляются абсолютно прозрачно.

**Ускоренный ввод/вывод**

Благодаря использованию в Hyper-V синтетических драйверов, которые не требуют дополнительной эмуляции виртуальных устройств, обмен данными при операциях ввода/вывода происходят гораздо быстрее по сравнению с традиционными решениями виртуализации. Максимального эффекта можно достичь при использовании в гостевых виртуальных машинах операционных систем Windows Server 2008 и Windows Vista с установленными в них драйверами синтетических устройств. В такой конфигурации находят, в частности применение синтетические драйверы для сетевых адаптеров и адаптеров памяти, тесно взаимодействующие с Windows-API. Это позволяет Hyper-V осуществлять быстрое преобразование I/O-запросов от гостевых систем в I/O-запросы к физическому оборудованию на родительском разделе.

Используя соответствующие компоненты интеграции, синтетические драйверы могут применяться также в отличных от Windows операционных системах (таких, как, например, использующие XEN операционные системы Linux). Для гостевых систем, не имеющих компонентов интеграции, Hyper-V в дочерних разделах осуществляет эмуляцию оборудования (например, сетевого адаптера) по тому же принципу, как и в других традиционных решениях виртуализации.

**Гостевые операционные системы: многообразие и совместимость**

На одном хост-сервере могут работать одновременно как 32-разрядные, так и 64-разрядные операционные системы (Windows, Linux и т. д.). В качестве гостевых систем Hyper-V, наряду с Windows Server 2008, Windows Vista SP1, Windows Server 2003 SP2 и Windows XP SP3, могут быть не относящиеся к Windows операционные системы (например, Novell, SUSE Linux). Таким образом, за счет интероперабельности Hyper-V компании могут консолидировать гетерогенную инфраструктуру и воспользоваться всеми преимуществами виртуализации как для Windows, так и для других ОС.

**Высокая доступность**

Вместе с отказоустойчивой кластеризацией Server 2008 Hyper-V упрощает восстановление виртуальных машин, размещенных на хранилищах SAN, после сбоя оборудования сервера, на котором они работают. В случае непредвиденного перерыва в работе хост-сервера, на котором функционируют виртуальные машины, вследствие отказа аппаратного обеспечения или вследствие проведения работ по техническому обслуживанию, соответствующие виртуальные машины автоматически запускаются на другом серверном узле кластера. Таким образом, на предприятии повышается доступность ИТ-сервисов.

**Управление**

Продукты на основе технологии Hyper-V отлично интегрируются в ИТ-инфраструктуру предприятия, поскольку для их настройки, резервного копирования и мониторинга можно использовать инструменты Microsoft System Center. Посредством WMI-интерфейса, а также Windows PowerShell можно индивидуально адаптировать решения Hyper-V и осуществлять их интеграцию в собственные процессы. Hyper-V позволяет использовать единые инструменты для обеспечения унифицированного управления как физическими, так и виртуальными ИТ-инфраструктурами, например, посредством Microsoft SCVMM и Microsoft SCDPM. С помощью средства PowerShell, содержащегося в Server 2008, можно осуществить полную отладку сценариев Hyper-V и SCVMM. Это позволяет осуществлять эффективную автоматизацию. Например, при слишком высокой загрузке физического хоста можно автоматически переместить

работающую на нем виртуальную машину из System Center Operations Manager 2007 на другой хост. Точно так же, с помощью SCVMM, возможно выполнить автоматическую конвертацию физических компьютеров в виртуальные машины.

#### 2.2.3.11 Кластеризация

В Server 2008 используется две технологии кластеризации. Кластеризация (clustering) – это группирование независимых серверных узлов, позволяющее получать доступ к этим серверам и просматривать их в сети так, будто бы они являются единой системой. Когда служба и/или приложение запускается из кластера, запросы подключающихся к нему пользователей могут обрабатываться, как только одним конкретным узлом, так и несколькими разными узлами кластера. В случае данных, доступных только для чтения, клиент может делать запрос к какому-то одному серверу в кластере, а его следующий запрос − направляться уже к другому серверу, причем так, что клиент об этом может даже и не догадываться. Кроме того, если один из узлов в кластере с несколькими узлами выйдет из строя, остальные узлы будут продолжать обслуживать клиентские запросы, и лишь те клиенты, которые были изначально подключены к вышедшему из строя узлу, могут либо заметить незначительный перерыв в обслуживании, либо вынуждены заново запустить свой сеанс, в зависимости от используемого ими приложения и того, какая технология кластеризации применяется в данном кластере.

Первой технологией кластеризации, которая используется в Server 2008, является отказоустойчивые кластеры. Отказоустойчивые кластеры (Failover Clusters) обеспечивают отказоустойчивость на уровне системы с помощью процесса, называемого подхватом функций (Failover). Когда какая-нибудь система или узел в кластере выходит из строя или перестает отвечать на запросы клиентов, кластеризованные службы или приложения, которые функционировали на этом конкретном узле, переводятся в автономный режим и перемещаются на другой узел, где снова делаются функциональными доступными. В большинстве реализаций отказоустойчивые кластеры требуют доступа к общему хранилищу данных и больше всего подходят (но не ограничиваются) для; развертывания перечисленных ниже приложений и служб.

– **Файловые серверы**. Файловые серверы в отказоустойчивых кластерах предоставляют почти все те функциональные возможности, которые может

предоставить автономная система Server 2008, но только при развертывании в виде кластеризованного сервера. Они позволяют создавать единый репозиторий хранилища данных и делать так, чтобы клиенты могли получать к нему доступ через назначенный и доступный в текущий момент узел без репликации данных файлов.

– **Серверы печати.** Службы печати, развертываемые в отказоустойчивых кластерах, обладают одним главным преимуществом по сравнению с автономными серверами печати: в случае выхода сервера печати из строя каждый из общих принтеров делается доступным для клиентов с тем же именем сервера печати. Хотя развертывание и замена принтеров для компьютеров и пользователей легко осуществляется с помощью групповых политик, последствия выхода из строя автономных серверов печати могут оказаться огромными, особенно когда доступ к этим принтерам получают такие серверы, устройства, службы и приложения, которыми нельзя управлять с помощью групповых политик.
– **Серверы баз данных.** При развертывании в крупных организациях производственных приложений, приложений электронной коммерции или других критически важных служб или приложений, требующих наличия вспомогательной системы баз данных с высокой степенью надежности, развертывание серверов − заданных в отказоустойчивых кластерах является предпочитаемым методом.
– **Вспомогательные производственные системы обмена сообщениями.** По многим таким же причинами, что перечислялись выше для серверов баз данных, службы обмена сообщениями стали играть во многих организациях критически важную роль и потому тоже больше всего подходят для развертывания в отказоустойчивых кластерах.

Вторая используемая в Server 2008 технология кластеризации называется технологией балансировки сетевой нагрузки − NLB. Эта технология больше всего подходит для обеспечения отказоустойчивости для интерфейсных Web-приложений и Web-сайтов, терминальных серверов (Terminal Servers), серверов VPN, серверов потоковых мультимедийных данных и прокси-серверов. Она обеспечивает

отказоустойчивость за счет того, что вынуждает каждый сервер в кластере индивидуально запускать сетевые службы и приложения и тем самым исключает вероятность появления одиночных точек сбоя. В зависимости от конкретных потребностей развертываемой в кластере NLB службы или приложения, для указания того, как клиенты будут подключаться к вспомогательным узлам кластера NLB, могут настраиваться опции конфигурации и сходства. Например, в случае доступного для чтения Web-сайта запросы клиентов могут направляться любому из узлов кластера NLB, из-за чего, следовательно, даже во время одного посещения этого Web-сайта клиент сможет подключаться к разным узлам кластера NLB. Другим примером служить приложение электронной коммерции, позволяющее клиентам приобретать товары или услуги, предоставляемые посредством Web-приложения из кластера NLB. В случае такого приложения сеанс каждого клиента должен инициироваться и обслуживаться только каким-то одним узлом в кластере, поскольку он наверняка будет подразумевать применение SSL − протокола безопасных соединений, а также содержать специфические сеансовые данные вроде содержимого корзины для виртуальных покупок и информации о конкретном пользователе, делающем эти покупки.

Microsoft не поддерживает возможность использования отказоустойчивых кластеров и кластеров NLB на одной и той же системе Server 2008.

#### 2.2.3.12 Результирующий набор политик

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

#### 2.2.3.13 Центр безопасности Windows

Центр безопасности Windows сводит в единое целое всю информацию о состоянии безопасности на компьютере и отправляет пользователю специальные сообщения о необходимости обновления приложений, предназначенных для обеспечения безопасности, и наличии в параметрах безопасности потенциально уязвимых мест, которые следует устранить. Так, в центре безопасности WSC может отображаться состояние параметров

межсетевого экрана и сведения о том, настроен ли компьютер на автоматический прием обновлений от корпорации Microsoft. Кроме того, этот компонент осуществляет мониторинг приложений для защиты от вирусов и шпионских программ, оповещая пользователя, если такие приложения отсутствуют или требуют обновления. Проверяются также параметры безопасности Internet Explorer и функции контроля учетных записей пользователей. Если они являются недостаточно надежными, центр безопасности Windows сообщает об этом пользователю и предоставляет рекомендации по устранению проблемы.

### 2.2.4 Основные функциональные возможности обеспечения безопасности при межсетевом взаимодействии

#### 2.2.4.1 Контролируемый доступ из сети

Операционная система Server 2008 располагает встроенными средствами безопасности, позволяющими препятствовать несанкционированному вторжению. Это достигается путем ограничения привилегий тех субъектов, которые пытаются получить удаленный доступ к компьютеру, до уровня «гость». Функционирование ОС Server 2008 базируется на ограничении прав любого, кто попытается осуществить доступ к компьютеру и получить несанкционированные привилегии путем подбора паролей, доступ данных субъектов будет либо невозможен, либо субъект получит только ограниченный доступ на уровне «гостя».

Операционная система Server 2008 по умолчанию сопоставляет всех пользователей, осуществляющих удаленный доступ, с учетной записью «гость». Таким образом, предотвращаются попытки злоумышленников получить удаленный доступ к компьютеру посредством локальной учетной записи администратора ОС Server 2008, не имеющей пароля.

#### 2.2.4.2 Брандмауэр сетевых подключений

Операционная система Server 2008 обеспечивает защиту доступа в сети средствами встроенного брандмауэра сетевых подключений (Internet Connection Firewall). Брандмауэр сетевых подключений обеспечивает защиту компьютера с установленной ОС Server 2008, непосредственно подключенного к сети, или персональных компьютеров и устройств,

подключенных к компьютеру с установленной ОС Server 2008, через который осуществляется общий доступ к внешним сетям.

В брандмауэре сетевых подключений реализован механизм активной фильтрации пакетов, порты брандмауэра открываются динамически только на время, необходимое для получения доступа к запрашиваемым услугам. Данная технология противодействует попыткам сканирования портов и ресурсов и прочих активов компьютера, в том числе папок и принтеров с общим доступом. При этом существенно снижается угроза внешних атак.

Брандмауэр сетевых подключений поддерживает подключения по коммутируемым каналам, локальной сети и по протоколу Point-to-Point over (через) Ethernet.

При включении брандмауэр сетевых подключений блокирует все несанкционированные подключения, поступающие через интерфейс внешней сети. Для этой цели в брандмауэре используется 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. Таким образом, если обмен информацией не санкционирован, входящий трафик блокируется.

В операционной системе Server 2008 реализована интеграция IPSec и новой версии брандмауэра, что позволило повысить сетевую производительность.

#### 2.2.4.3 Поддержка стандартов безопасности

Операционная система Server 2008 обеспечивает возможность поддержки безопасных вычислительных сетей, построенных на основе таких стандартов безопасности как IPSec (Internet Protocol Security) и Kerberos v.5 rev.6.

***IP-безопасность (IPSec)***

IP-безопасность интегрирована со стеком TCP/IP и обеспечивает защиту IP-данных от перехвата и несанкционированных манипуляций, а также защиту от сетевых атак различных типов. Использование прокола IPSec позволяет обеспечить безопасность данных, передаваемых по сети. Протокол безопасности IPSec играет важную роль в

обеспечении безопасности виртуальных частных сетей (VPN), обеспечивающих возможность безопасной передачи данных через менее доверенные вычислительные сети.

***Поддержка протокола аутентификации Kerberos***

В ОС Server 2008 аутентификационные данные пользователя могут быть представлены в виде пароля, мандата Kerberos или смарт-карты, если компьютер оборудован для работы со смарт-картами.

Протокол аутентификации Kerberos обеспечивает средства взаимной проверки подлинности клиентов, например пользователя, компьютера или службы и сервера. Используя поддержку протокола Kerberos v.5 rev.6 ОС Server 2008 предоставляет пользователям возможность однократного ввода аутентификационных данных для доступа ко всем активам и поддерживаемым приложениям, права на доступ, к которым у них имеются.

***Защищенные беспроводные сети***

Операционная система Server 2008 обеспечивает поддержку стандарта IEEE 802.1X, позволяющего усилить безопасность и повысить эффективность развертывания вычислительной сети за счет централизации идентификации пользователей, проверки их подлинности, динамического управления ключами сети WEP (Wired Equivalent Privacy) и управления учетными записями.

**2.2.4.4 Microsoft Internet Explorer в защищенном режиме**

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

Для защиты пользовательских данных Internet Explorer содержит:

- фильтр фишинга, формирующий предупреждение пользователю о подозрительных web-узлах, выполняющих несанкционированный сбор конфиденциальной информации;

– строку состояния безопасности, содержащую сведения о безопасности и надежности web-узлов;
– адресную строку во всех окнах, предоставляющую пользователям получить сведения об истинном источнике информации.

## 2.3Среда функционирования и границы ОО

### 2.3.1 Конфигурации ОО

Объект оценки функционирует в следующих конфигурациях:

– **Enterprise Client (EC);**
– **Specialized Security Limited Functionality (SSLF**).

### 2.3.2 Среда функционирования

Возможная среда функционирования ОО определяется конфигурациями **«Enterprise Client» (EC)** и «**Specialized Security – Limited Functionality» (SSLF).**

**Enterprise Client**

Данная среда функционирования предусматривает развернутую инфраструктуру домена на базе службы каталогов Microsoft Active Directory, включающей в свой состав клиентские компьютеры только под управлением ОС Microsoft Windows Vista SP1 и/или ОС Microsoft Windows XP с SP3.

В качестве рядовых серверов в данной конфигурации могут использоваться только компьютеры с установленной ОС Server 2008 и/или ОС Microsoft Windows Server 2003 с SP2. Роль контроллеров домена в указанной конфигурации выполняют компьютеры под управлением ОС Server 2008. Управление серверами и клиентскими компьютерами в данной конфигурации происходит через использование групповой политики, применяемой на различных уровнях иерархии службы каталогов Active Directory (сайты, домены, организационные подразделения) и предоставляющей механизм централизованного управления политиками безопасности для среды функционирования в целом.

**Specialized Security – Limited Functionality**

Конфигурация «**Specialized Security – Limited Functionality**» по сравнению с конфигурацией «Enterprise Client» подразумевает наличие более ограничивающей политики безопасности и усиленные настройки безопасности для серверов только под управлением ОС Server 2008. Конфигурация «**Specialized Security – Limited Functionality**» предусматривает ограничение функциональных возможностей пользователя полномочиями на выполнение только необходимых ему задач.

Данная конфигурация предусматривает наличие клиентских компьютеров под управлением ОС Microsoft Windows Vista SP1 и/или ОС Microsoft Windows XP с SP3. В качестве рядовых серверов и контроллеров домена в данной конфигурации могут использоваться только компьютеры под управлением ОС Server 2008.

### 2.3.3 Роли серверов

Server 2008 может выполнять следующие роли:

- служба доменов Active Directory (AD DS), хранит информацию о пользователях, компьютерах и других устройствах в сети. AD DS помогает администраторам надежно управлять этой информацией и облегчает разделение ресурса и взаимодействия между пользователями;
- облегченная служба каталогов Active Directory (AD LDS), позволяет производить развертывание служб каталогов для приложений, ориентированных на работу с каталогами, используя их как хранилище данных;
- служба управления правами Active Directory (AD RMS) – информационная технология защиты, предназначенная для защиты информации пользователей от несанкционированного доступа;
- служба федерации Active Directory (AD FS) позволяет обеспечивать возможность осуществления единого входа – SSO между несколькими платформами и не-Microsoft средами, включительно;
- служба сертификации Active Directory (AD CS), предоставляет настраиваемый сервис для создания и управления общих ключей сертификатов, используемых в системах безопасности программного обеспечения с применением технологий

общих ключей; не включены: служба подачи заявок на регистрацию сетевых устройств (NDES) и служба сетевого ответчика (Online Responder);

- Hyper-V – гипервизорная технология создания виртуальных машин в ОС Server 2008;
- сервер приложений (Application Server), обеспечивает создание законченных решений для предоставления услуг по размещению информации и управлению высокоэффективными распределенными бизнес-приложениями;
- сервер протокола динамической настройки узлов (Dynamic Host Configuration Protocol), позволяет компьютерам и другим устройствам в сети автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP;
- сервер служб доменных имен (Domain Name Service), реализует стандартный метод сопоставления доменных имен с интернет-адресами;
- сервер факсов (Fax Server), посылает и получает факсимильные сообщения и позволяет управлять факс-ресурсами, такими как рабочие места, параметрами настройки, сообщениями и факсимильными устройствами, установленными на компьютере или в сети;
- файловая служба (File Services) предоставляет технологию управления внешней памятью, репликации файлов, управления распределенным пространством имен, обеспечивает быстрый поиск файлов и рационализированный доступ к файлам, поддерживает только один корень пространства имен DFS (DFS root);
- служба сетевых политик и доступа (Network Policy and Access Services), предоставляет пользователям различные способы локального и удаленного сетевого соединения, соединения сегментов сети и позволяет администраторам сети централизованно управлять доступом в сети и политикой безопасности клиента;
- служба печати (Print Services), обеспечивает управление серверами печати и принтерами, уменьшая административные и рабочие нагрузки управления за счет централизации задач управления;
- терминальная служба (Terminal Services), предоставляет пользователям доступ к Windows-базируемым программам, установленным на сервере терминалов, или доступ к рабочему столу любого компьютера. Пользователь может

соединиться с сервером терминалов для выполнения программы и использования ресурсов этого сервера;

- службы универсального описания, обнаружения и интеграции (UDDIS) – инструмент для расположения описаний Web-сервисов (WSDL) для последующего их поиска другими организациями и интеграции в свои системы;
- Web-сервер позволяет обеспечивать обмен информацией в Интернете, интранете или экстранете;
- службы развертывания Windows (Windows Deployment Services), позволяют устанавливать и конфигурировать Windows операционные системы на удаленных компьютерах из PXE boot ROMs;
- служба обновления серверов WSUS, предназначена для получения актуальных пакетов и индивидуальных обновлений непосредственно с Microsoft.

В каждой роли имеется ряд служб, которые и составляют роль. Службы роли позволяют администратору загружать только те службы, которые нужны для данного конкретного сервера.

В дополнение к ролям и службам ролей, в Server 2008 имеется возможность добавлять компоненты. Компоненты предназначены для поддержки ролей или служб ролей, но не зависят от них. В Server 2008 имеется много различных компонентов, часть из которых перечислена ниже:

- Microsoft .NET Framework 3.0 Features (компоненты .NET Framework 3.0);
- BitLocker Drive Encryption (шифрование диска BitLocker);
- BITS Server Extensions (серверные расширения BITS);
- Connection Manager Administration Kit (CMAK) (инструментальный набор администрирования диспетчера подключений);
- Desktop Experience (среда рабочих столов);
- Failover Clustering (кластеризация подхвата);
- Group Policy Management (управление групповыми политиками);
- Internet Printing Client (клиент Интернет–печати);
- Internet Storage Name Server (iSNS) (сервер имен Интернет–хранилища данных, iSNS);
- LPR Port Monitor (LPR) (монитор портов LPR);

- Message Queuing (служба очередей сообщений);
- Multipath I/O (MPIO) (разветвленный ввод/вывод);
- Network Load Balancing (балансировка сетевой нагрузки;
- Peer Name Resolution Protocol (PNRP) (протокол разрешения сетей в одноранговых сетях);
- Quality Windows Audio Video Experience (qWave) (среда качественного аудио и видео Windows, qWave);
- Remote Assistance (удаленный помощник);
- Remote Server Administration Tools (средства администрирования удаленного сервера);
- Remote Differential Compression (удаленное разностное сжатие);
- Removable Storage Manager (RSM) (диспетчер сменных носителей);
- RPC Over HTTP Proxy (прокси RPC поверх HTTP);
- Simple TCP/IP Services (служба простого TCP/IP);
- SMTP Server (сервер SMTP);
- Simple Network Management Protocol (SNMP) Services (служба SNMP);
- Storage Manager for Storage Area Networks (SANs) (диспетчер памяти для сетей SAN);
- Subsystem for UNIX–based Applications (подсистема для UNIX-приложений);
- Telnet Client (клиент Telnet);
- Telnet Server (сервер Telnet);
- Trivial File Transfer Protocol (TFTP) Client (клиент TFTP);
- Windows Internal Database (внутренняя база данных Windows);
- Windows PowerShell – интегрированная оболочка выполнения команд и язык написания сценариев;
- Windows System Resource Manager (WSRM) (диспетчер системных ресурсов Windows);
- Windows Internet Naming Service (WINS) (сервер WINS);
- Windows Process Activation Service (WPAS) (служба активации процессов Windows);

– Windows Server Backup Features (компонент резервного копирования сервера Windows);
– Wireless LAN (WLAN) Service (служба беспроводной LAN).

### 2.3.4 Логические границы ОО

Объект оценки – это модульная система, состоящая из программных компонентов, работающих либо в непривилегированном режиме процессора (пользовательском режиме), либо в привилегированном режиме процессора (режиме ядра) и совместно выполняющих разные задачи. Каждый компонент ОО реализует определенные функции, которые служат своеобразным интерфейсом для остальной части системы (см. рисунок 2.1).

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

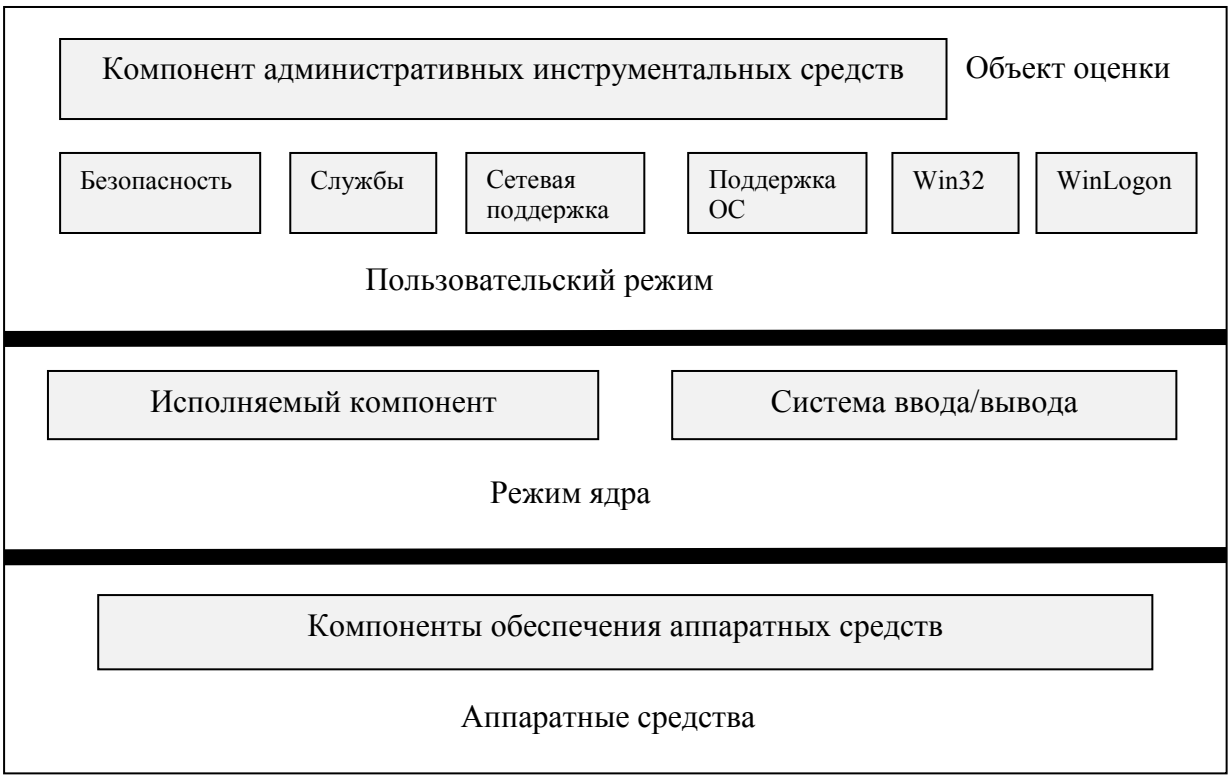



Рисунок 2.1 – Структурная схема ОО

Компоненты системы объекта оценки:

- Модуль инструментальных средств администратора:
  - компонент административных инструментальных средств (GUI компонент), предназначен для управления свойствами безопасности ФБО;
- Модуль безопасности:
  - компонент безопасности, включает в себя все службы и функции управления безопасностью;
- Модуль служб:
  - компонент служб, обеспечивает систему сервисом контроля;
- Модуль сетевой поддержки и процедуры удаленного вызова (RPC):
  - компонент сетевой поддержки, имеет в своем составе службу поддержки RPC, COM и другие услуги сети;
- Модуль поддержки ОС:
  - компонент поддержки ОС, представляет ряд процессов, обеспечивающих поддержку функций и сервисов других ОС;
- Модуль Win32:
  - компонент Win32 обеспечивает поддержку сервиса Win32-приложений и приложения консоли командной строки;
- Модуль WinLogon:
  - компонент WinLogon, предоставляет: различные диалоговые услуги входа в систему, включая аутентификацию, доверенный путь, управление сессиями и блокировку;
- Программное обеспечение модуля ядра:
  - исполняемый компонент является программным обеспечением режима ядра, которое обеспечивает ядро ОС сервисами, включающими в себя управление памятью, управление процессами и связями между ними;
  - система ввода/вывода является программным обеспечением режима ядра, которое реализует все сервисы, связанные с вводом/выводом, включая драйвера, обеспечивающие процессы ввода/вывода. Система ввода/вывода состоит из следующих компонентов:
    - компонент в/в ядра;

  - компонент в/в файла;
  - компонент в/в сети;
  - компонент в/в устройств.
- Модуль аппаратных средств:

  Компонент аппаратных средств содержит все аппаратные средства, включая процессор(ы), системную плату и связанные с ней чип сеты, контроллеры и устройства ввода/вывода.

### 2.3.5 Физические границы ОО

Физические границы ОО включают персональный компьютер со следующими минимально необходимыми аппаратными характеристиками:

- процессор семейства Intel x86 (32-бит и 64-бит) минимально – 1ГГц, (рекомендуется – 2ГГц, оптимально – 3ГГц и выше);
- минимальный объем оперативной памяти – 512 Мбайт, рекомендуемый объем – 1 ГБ, оптимально – 2 ГБ, максимум для 32-разрядных систем – 64 ГБ, для 64-разрядных систем − 2 ТБ;
- не менее 8 ГБ свободного дискового пространства (рекомендуемый объем – 40 ГБ, оптимально – 80 ГБ);
- видеоадаптер и монитор для работы в режиме SVGA 800x600;
- привод DVD-ROM;
- клавиатура и мышь;
- сетевой адаптер.

## 2.4Службы безопасности ОО

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

### 2.4.1 Аудит безопасности

Объект оценки обеспечивает выявление и запись данных о событиях, существенных с точки зрения безопасности, а также предоставляет средства для анализа

записей о таких событиях. Перечень типов событий, подлежащих регистрации, определяется администратором ОО и может детализироваться вплоть до доступа к конкретным файлам или каталогам отдельных пользователей или групп. После настройки параметров аудита можно отслеживать доступ пользователей к определенным объектам и анализировать недостатки системы безопасности. Записи аудита, содержащие сведения по выбранным событиям, содержат информацию о пользователе, который был инициатором события и выполнял какие-либо действия в отношении контролируемого объекта, а также дату, время события и другие данные. ОО обеспечивает возможность доступа к журналу аудита только уполномоченным на это пользователям.

Объект оценки обеспечивает защиту данных аудита от потери, используя возможность аварийного завершения работы системы при условии невозможности внесения в журнал аудита записи о событиях безопасности по причине отсутствия доступного дискового пространства.

### 2.4.2 Защита данных пользователя

Объект оценки осуществляет функции и политику избирательного (дискреционного) управления доступом, фильтрацию информации, а также реализует механизм защиты остаточной информации. Избирательное управление доступом предоставляет возможность ограничивать и контролировать доступ к системе, приложениям и ресурсам, таким как файлы, папки, принтера и объекты службы каталогов Active Directory. Каждый пользователь, пытающийся получить доступ к системе, сначала проходит процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, – авторизацию, т.е. проверку разрешений пользователя по отношению к какому-либо защищаемому объекту. Вся информация, определяющая безопасность защищаемого объекта, хранится в ассоциированном с ним дескрипторе безопасности, который формируется при создании объекта и впоследствии может меняться. Изменять содержимое дескриптора безопасности могут пользователи, имеющие статус владельца объекта, а также субъекты, которым предоставлены соответствующие полномочия. Главными компонентами дескрипторами безопасности объекта являются дискреционный список управления доступом DACL (Discretional Access Control List), который собственно и определяет права доступа к объекту, и системный список контроля доступа SACL (System Access Control List), служащий для назначения аудита.

Объект оценки обеспечивает фильтрацию входящей в ОО информации (защиту доступа в сети) с использованием брандмауэра сетевых подключений. ОО также обеспечивает защиту данных пользователя посредством механизма, обеспечивающего обезличивание (обнуление) остаточной информации в свободных блоках памяти (оперативной и дисковой) перед их предоставлением каким-либо процессам, выполняющимся в режиме пользователя.

### 2.4.3 Идентификация и аутентификация

Объект оценки требует, чтобы все 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 локальную базу данных (БД) и каталог безопасности (хранилище Active Directory), хранящие информацию об учетных записях пользователей. Каждая учетная запись представлена идентификатором пользователя, однозначно связанным с его идентификатором безопасности – SID (Security Identifier), аутентификационной информацией, информацией о членстве в группах безопасности, ассоциированными правами и полномочиями (привилегиями). ОО обеспечивает хранение паролей в преобразованном формате. ОО предоставляет средства усиления безопасности паролей через использование механизма политик безопасности, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля. ОО предоставляет механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором ОО или по истечении времени действия, заданного для счетчика блокировки.

### 2.4.4 Управление безопасностью

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

Объект оценки поддерживает возможность тиражирования (реплицирования) всех изменений, связанных с безопасным состоянием ОО (блокирование учетной записи, изменение пароля доступа и др.), на все серверы, выполняющие роль контроллеров домена.

### 2.4.5 Защита ФБО

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

### 2.4.6 Использование ресурсов ОО

Объект оценки может ограничивать объем доступного для пользователя дискового пространства посредством использования механизма дисковых квот. Дисковые квоты используются для управления объемом хранимых данных и позволяют распределять дисковое пространство между пользователями в зависимости от того, владельцами каких папок и файлов они являются. ОО позволяет учитывать дисковые квоты для каждого тома, даже если эти тома расположены на одном и том же жестком диске. По умолчанию только члены группы «Администраторы» (Administrators) могут устанавливать дисковые квоты, определять пороги выдачи предупреждений и пределы квот как для всех пользователей, так и индивидуально для каждого пользователя. Кроме того, администратор ОО

уполномочен определять действия, выполняемые системой при превышении квот пользователями.

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

### 2.4.7 Блокирование сеанса

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

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

### 2.4.8 Управление доступом к ОО

Объект оценки предоставляет возможность ограничения открытия сеанса доступа на основе идентификатора пользователя, времени доступа, имени компьютера, с которого осуществляется доступ к ОО, и срока действия аутентификационных данных.

# 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.ImpossibleModif**

Должно быть обеспечено отсутствие на ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

**A.ConnectTOE**

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

**A.TOEConfig**

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

**A.TrustedLoad**

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

**A.DisableDebugger**

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

**A.UsagePrint**

При осуществлении печати документов должна быть обеспечена регистрация краткого содержания (наименование, вид, шифр, код) выдаваемого на печать документа.

**A.RegistrDisk**

Должен быть обеспечен учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в соответствующий, предусмотренный для этой цели журнал.

**A.StorageClearing**

Должна быть обеспечена очистка (обнуление, обезличивание) освобождаемых внешних накопителей путем однократной произвольной записи в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

**A.IntegrityControl**

Должна быть обеспечена надлежащая периодическая проверка целостности программного обеспечения ОО.

### 3.1.2 Предположения относительно среды функционирования ОО

**Предположение, связанное с физической защитой ОО**

**A.LocateTOE**

Для предотвращения несанкционированного физического доступа к ОО, он должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

**Предположения, имеющие отношение к персоналу**

**A.NoEvilAdm**

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

**A.NoEvilUser**

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, руководствоваться в своей работе эксплуатационной документацией на ОО, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

**Предположения связности**

**A.SinglePoint**

При использовании брандмауэра сетевых подключений необходимо обеспечить, чтобы ОО являлся единственной точкой доступа в защищаемую внутреннюю вычислительную сеть из внешней вычислительной сети.

**A.SystemInteraction**

Все системы ИТ, с которыми ОО осуществляет взаимодействие, должны идентифицироваться на основе логических имен.

## 3.2 Угрозы

В настоящем ЗБ определены следующие угрозы, которым противостоит ОО.

**T.UnauthAccessData**

**1. Аннотация угрозы –** осуществление доступа к пользовательским данным неуполномоченными на это пользователями ОО.

**2. Источники угрозы –** пользователи ОО.

**3. Способ реализации угрозы –** осуществление доступа к пользовательским данным локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

**4. Используемые уязвимости –** недостатки механизмов разграничения доступа к пользовательским данным, связанные с возможностью предоставления доступа к пользовательским данным неуполномоченным на это пользователям ОО.

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

**6. Нарушаемые свойства безопасности активов –** конфиденциальность, целостность, достоверность, доступность.

**7. Возможные последствия реализации угрозы –** несанкционированное ознакомление с пользовательскими данными; несанкционированная модификация (в том числе подмена) пользовательских данных; несанкционированное удаление пользовательских данных.

**T.UnauthExecProg**

**1. Аннотация угрозы –** осуществление доступа и выполнение исполняемых программ неуполномоченными на это пользователями ОО.

**2. Источники угрозы –** пользователи ОО.

**3. Способ реализации угрозы –** осуществление доступа и выполнение исполняемых программ локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

**4. Используемые уязвимости –** недостатки механизмов разграничения доступа к исполняемым программам, связанные с возможностью доступа и выполнения исполняемых программ неуполномоченными на это пользователями ОО.

**5. Вид активов, потенциально подверженных угрозе –** исполняемые программы.

**6. Нарушаемое свойство безопасности активов –** несанкционированное выполнение.

**7. Возможные последствия реализации угрозы –** несанкционированное ознакомление с информацией, выдаваемой после отработки исполняемых программ; нарушение режимов функционирования ОО.

**T.UnauthAccessTOE**

**1. Аннотация угрозы –** осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся на объектах ОО (файлах, папках, и т.п.).

**2. Источники угрозы –** сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем (в том числе ОС)).

**3. Способ реализации угрозы –** осуществление удаленного доступа к ОО с использованием средств, поддерживающих возможность взаимодействия с ОО.

**4. Используемые уязвимости –** недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО; пользовательские данные.

**6. Нарушаемые свойства безопасности активов –** целостность, подконтрольность, конфиденциальность.

**7. Возможные последствия реализации угрозы –** нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и пользовательскими данными.

**T.MasqAdmin&User**

**1. Аннотация угрозы –** осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого пользователя ОО или администратора ОО.

**2. Источники угрозы –** пользователи ОО; администраторы ОО.

**3. Способ реализации угрозы –** осуществление доступа к ОО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

**4. Используемые уязвимости –** недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО; пользовательские данные.

**6. Нарушаемые свойства безопасности активов –** целостность, подконтрольность, конфиденциальность.

**7. Возможные последствия реализации угрозы –** нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и пользовательскими данными; невозможность однозначного сопоставления совершенных в ОО действий с пользователем, совершившим данные действия.

**T.UnauthAccessAudit**

**1. Аннотация угрозы –** осуществление доступа к данным аудита ОО пользователями ОО и неуполномоченными на это администраторами ОО и возможность несанкционированного удаления и модификации данных аудита ОО.

**2. Источники угрозы –** пользователи ОО; администраторы ОО.

**3. Способы реализации угрозы –** осуществление доступа к данным аудита ОО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

**4. Используемые уязвимости –** недостатки механизмов разграничения доступа к данным аудита, связанные с возможностью осуществления доступа к данным аудита пользователями ОО и неуполномоченными на это администраторами ОО.

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

**6. Нарушаемые свойства безопасности активов –** подконтрольность, целостность, конфиденциальность.

**7. Возможные последствия реализации угрозы –** невозможность осуществления контроля действий пользователей ОО и администраторов ОО, а также контроля процесса функционирования ОО в целом; навязывание администраторам ОО, ответственным за контроль данных аудита ОО, ложных (модифицированных) данных аудита; несанкционированное ознакомление о произошедших в ОО событиях.

**T.LostAudit**

**1. Аннотация угрозы –** потеря данных аудита ОО вследствие переполнения выделенного для задач аудита хранилища информации.

**2. Источники угрозы –** события, подвергаемые аудиту.

**3. Способ реализации угрозы –** переполнение выделенного для задач аудита хранилища информации.

**4. Используемые уязвимости –** недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за переполнения хранилища данных аудита ОО.

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

**6. Нарушаемые свойства безопасности активов –** целостность.

**7. Возможные последствия реализации угрозы –** невозможность осуществления контроля произошедших в ОО событий.

**T.UnauthAccessTSF**

**1. Аннотация угрозы –** осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами ОО.

**2. Источники угрозы –** пользователи ОО; администраторы ОО.

**3. Способ реализации угрозы –** осуществление доступа к данным ФБО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

**4. Используемые уязвимости –** недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО.

**6. Нарушаемые свойства безопасности активов –** конфиденциальность, целостность, доступность, достоверность.

**7. Возможные последствия реализации угрозы –** несанкционированное ознакомление с данными ФБО (конфигурационные файлы, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

**T.UsageSession**

**1. Аннотация угрозы –** осуществление доступа к ОО и защищаемым активам неуполномоченными пользователями ОО или администраторами ОО путем использования открытой сессии, незавершенной во время работы с ОО другим уполномоченным пользователем ОО или администратором ОО.

**2. Источники угрозы –** пользователи ОО; администраторы ОО.

**3. Способ реализации угрозы –** использование открытой сессии, незавершенной во время работы с ОО другим уполномоченным пользователем ОО или администратором ОО.

**4. Используемые уязвимости –** недостатки механизмов разграничения доступа к ОО, связанные с возможностью использования открытой сессии, незавершенной во время работы с ОО другим уполномоченным пользователем ОО или администратором ОО.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО; пользовательские данные.

**6. Нарушаемые свойства безопасности активов –** целостность, подконтрольность, конфиденциальность.

**7. Возможные последствия реализации угрозы –** нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и пользовательскими данными.

**T.UnauthUsageRes**

**1. Аннотация угрозы –** исчерпание свободных ресурсов ОО (вычислительные возможности, дисковое пространство) вследствие неограниченного их использования пользователями ОО.

**2. Источники угрозы –** пользователи ОО.

**3. Способ реализации угрозы –** генерация процессов, использующих вычислительны возможности ОО, и создание объектов, использующих дисковое пространство ОО, пользователями ОО.

**4. Используемые уязвимости –** недостатки механизмов надлежащего распределения ресурсов ОО, связанные с возможностью их исчерпания.

**5. Вид активов, потенциально подверженных угрозе –** ресурсы ОО.

**6. Нарушаемое свойство безопасности активов –** доступность.

**7. Возможные последствия реализации угрозы –** нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

**T.FailureTOE**

**1. Аннотация угрозы –** нарушение режимов функционирования ОО, а также потеря или искажение данных ФБО и пользовательских данных вследствие сбоев и отказов программного обеспечения и оборудования ОО.

**2. Источники угрозы –** программное обеспечение и оборудование ОО.

**3. Способ реализации угрозы –** сбои и отказы программного обеспечения и оборудования ОО.

**4. Используемые уязвимости –** недостатки механизмов защиты ОО от сбоев и отказов программного обеспечение и оборудования ОО; недостатки механизмов безопасного восстановления ОО после сбоев и отказов программного обеспечения и оборудования ОО.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО; пользовательские данные; программное обеспечение ОО.

**6. Нарушаемое свойство безопасности активов –** целостность, доступность.

**7. Возможные последствия реализации угрозы –** нарушение режимов функционирования ОО; потеря и искажение данных ФБО и пользовательских данных.

**T.FaultConformMng**

**1. Аннотация угрозы –** нарушение режимов взаимодействия ОО, управляемых клиентских и серверных ОС вследствие несогласованной интерпретации совместно используемых данных ФБО.

**2. Источники угрозы –** программное обеспечение ОО.

**3. Способ реализации угрозы –** несогласованность в интерпретации совместно используемых данных ФБО.

**4. Используемые уязвимости –** недостатки механизмов ОО, обеспечивающих согласованную интерпретацию совместно используемых данных ФБО.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО; пользовательские данные; программное обеспечение ОО.

**6. Нарушаемое свойство безопасности активов –** целостность, доступность.

**7. Возможные последствия реализации угрозы –** нарушение режимов взаимодействия ОО, управляемых клиентских и серверных ОС.

**T.FaultConformSrv**

**1. Аннотация угрозы –** нарушение режимов взаимодействия ОО и других экземпляров ОО, установленных на серверах для решения задач совместного с ОО обеспечения безопасности информации, вследствие несогласованной интерпретации совместно используемых данных ФБО.

**2. Источники угрозы –** программное обеспечение ОО.

**3. Способ реализации угрозы –** несогласованность в интерпретации совместно используемых данных ФБО.

**4. Используемые уязвимости –** недостатки механизмов ОО, обеспечивающих согласованную интерпретацию совместно используемых данных ФБО.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО; пользовательские данные; программное обеспечение ОО.

**6. Нарушаемое свойство безопасности активов –** целостность, доступность.

**7. Возможные последствия реализации угрозы –** нарушение режимов взаимодействия ОО и других экземпляров ОО, установленных на серверах для решения задач совместного с ОО обеспечения безопасности информации.

## 3.3 Политика безопасности организации

Объект оценки должен следовать приведенным ниже правилам политики безопасности организации.

**P.InteractOS**

В случае функционирования ОО, управляемых клиентских и серверных ОС, установленных на рабочих станциях пользователей и отдельных серверах, для совместного решения задач обеспечения безопасности информации должно быть обеспечено надлежащее взаимодействие ОО с управляемыми клиентскими и серверными ОС и реализована возможность управления настройками, определяющими ПФБ этих клиентских и серверных ОС.

**P.SynchrState**

В случае функционирования ОО и других экземпляров ОО, установленных на компьютерах, для совместного решения задач обеспечения безопасности информации и управления клиентскими и серверными ОС должна быть обеспечена возможность проведения надлежащей синхронизации состояния безопасности, вызванной изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО.

**P.AdminManage**

Должно быть обеспечено наличие надлежащих корректно функционирующих средств администрирования ОО, управляемых клиентских и серверных ОС, доступных только уполномоченным администраторам ОО. Уполномоченным пользователям ОО должна быть предоставлена возможность модификации собственных аутентификационных данных.

**P.AuditEvents**

Должны быть обеспечены надлежащая регистрация и предупреждение администратора ОО о любых событиях, относящихся к безопасности ОО. Должна быть обеспечена возможность для администратора ОО выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

**P.AccessAssets**

Должна быть обеспечена возможность для уполномоченных на это пользователей ОО определять доступность защищаемых активов для других пользователей ОО.

**P.TrustedPath**

Должна быть обеспечена невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

**P.FiltrationFlow**

Должна осуществляться фильтрация входящих в ОО информационных потоков.

**P.ResidualInform**

Должна быть обеспечена недоступность информационного содержания освобождаемой памяти, выделяемой процессам.

**P.TestFunctions**

Должна быть обеспечена возможность периодического контроля целостности ФБО и его данных, а также возможность регламентного тестирования ОО и среды функционирования ОО на предмет корректности функционирования.

**P.SOFAuth**

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

# 4 Цели безопасности

## 4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

**O.AccessAssets**

**Разграничение доступа к защищаемым активам**

ОО должен обеспечивать доступ к защищаемым активам только уполномоченным на это пользователям ОО и администраторам ОО. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО и администраторам ОО определять доступность защищаемых активов для других пользователей ОО и администраторов ОО.

**O.AccessTOE**

**Разграничение доступа к ОО**

ОО должен обеспечивать доступ к ОО только уполномоченным на это пользователям ОО и администраторам ОО. Должны быть предусмотрены механизмы блокирования сеанса пользователя ОО и администратора ОО, осуществляемого по их инициативе, а также инициируемого ФБО и основанного на интервале времени бездействия пользователя ОО или администратора ОО.

**O.InteractOS**

**Взаимодействие с управляемыми ОС**

В случае функционирования ОО, управляемых клиентских и серверных ОС, установленных на рабочих станциях пользователей и отдельных серверах, для совместного решения задач обеспечения безопасности информации ОО должен поддерживать надлежащее согласованное взаимодействие с управляемыми клиентскими и серверными ОС и обеспечивать возможность управления настройками, определяющими ПФБ этих клиентских и серверных ОС.

**O.SynchrState**

**Обеспечение синхронизации состояния безопасности**

В случае функционирования ОО и других экземпляров ОО, установленных на компьютерах, для совместного решения задач обеспечения безопасности информации ОО должен обеспечивать возможность проведения надлежащей согласованной

синхронизации состояния безопасности, вызванной изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО.

**O.AuditEvents**

**Аудит событий**

ОО должен располагать надлежащими механизмами регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации должны предоставлять уполномоченным администраторам ОО возможность выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

**O.ProtectAudit**

**Защита данных аудита**

ОО должен обеспечивать защиту данных аудита от несанкционированного использования, предоставляя доступ к данным аудита только уполномоченным администраторам ОО, и предотвращать потерю данных аудита в случае переполнения их хранилища.

**O.ResidualInform**

**Защита остаточной информации**

ОО должен обеспечивать недоступность информационного содержания освобождаемой памяти, выделяемой процессам.

**O.AdminManage**

**Наличие средств администрирования**

ОО должен располагать надлежащими корректно функционирующими средствами администрирования ОО, управляемых клиентских и серверных ОС, доступными только уполномоченным администраторам ОО. ОО должен предоставить для уполномоченных пользователей ОО возможность модификации собственных аутентификационных данных.

**O.ProtectTSF**

**Защита данных ФБО**

ОО должен обеспечивать защиту данных ФБО, поддерживая домен для функционирования ФБО.

**O.DistrResource**

**Надлежащее распределение ресурсов**

ОО должен обеспечивать для уполномоченного администратора ОО возможность надлежащего распределения дискового и процессорного ресурсов ОО.

**O.TrustedPath**

**Доверенная аутентификация**

ОО должен обеспечить невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

**O.FiltrationFlow**

**Фильтрация информационных потоков**

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

**O.SafeRecovery**

**Безопасное восстановление**

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

**O.TestFunctions**

**Контроль функционирования**

ОО должен предоставлять возможность периодического контроля целостности ФБО и его данных, а также возможность собственного регламентного тестирования и тестирования среды функционирования ОО на предмет корректности функционирования.

**O.SOFAuth**

**Стойкость функции безопасности**

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

## 4.2 Цели безопасности для среды

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

**OE.ImpossibleModif**

**Стерильность среды функционирования**

Должно быть обеспечено отсутствие на ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

**OE.ConnectTOE**

**Контролируемые точки доступа**

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

**OE.TOEConfig**

**Эксплуатация ОО**

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

**OE.LocateTOE**

**Физическая защита ОО**

Для предотвращения несанкционированного физического доступа к ОО, он должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

**OE.NoEvilAdm**

**Требования к администраторам ОО**

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

**OE.NoEvilUser**

**Требования к пользователям ОО**

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, руководствоваться в своей работе эксплуатационной документацией на ОО, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

**OE.TrustedLoad**

**Доверенная загрузка**

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

**OE.DisableDebugger**

**Отключение встроенных программ отладки**

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

**OE.SinglePoint**

**Единственная точка доступа**

При использовании брандмауэра сетевых подключений должно быть обеспечено, чтобы ОО являлся единственной точкой доступа в защищаемую внутреннюю вычислительную сеть из внешней вычислительной сети.

**OE.UsagePrint**

**Печать документов**

При осуществлении печати документов должна быть обеспечена регистрация краткого содержания (наименование, вид, шифр, код) выдаваемого на печать документа.

**OE.RegistrDisk**

**Учет носителей информации**

Должен быть обеспечен учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в соответствующий, предусмотренный для этой цели журнал.

**OE.StorageClearing**

**Очистка внешних накопителей**

Должна быть обеспечена очистка (обнуление, обезличивание) освобождаемых внешних накопителей путем однократной произвольной записи в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

**OE.IntegrityControl**

**Проверка целостности**

Должна быть обеспечена надлежащая периодическая поверка целостности программного обеспечения ОО, основанная на проведении контрольного суммирования программного обеспечения ОО.

**OE.SystemInteraction**

**Идентификация по логическим именам**

Должна быть обеспечена идентификация систем ИТ (серверных и клиентских ОС), с которыми ОО осуществляет взаимодействие, на основе логических имен.

# 5 Требования безопасности ИТ

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

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

## 5.1 Требования безопасности для ОО

### 5.1.1 Функциональные требования безопасности ОО

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности ОО, и сформулированные в явном виде, 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 |

| Идентификатор компонента требований | Название компонента требований |
|---|---|
| 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 |
| FDP_RIP.1 | Ограниченная 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 (EXT) | 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 |
| FPT_AMT.1 | Тестирование абстрактной машины |

| Идентификатор компонента требований | Название компонента требований |
|---|---|
| FPT_FLS.1 | Сбой с сохранением безопасного состояния |
| FPT_ITT.1 | Базовая защита внутренней передачи данных ФБО |
| FPT_RCV.1 | Ручное восстановление |
| FPT_RVM.1 | Невозможность обхода ПБО |
| FPT_SEP.1 | Отделение домена ФБО |
| FPT_SSP.1 | Одностороннее надежное подтверждение |
| FPT_STM.1 | Надежные метки времени |
| FPT_TDC.1 | Базовая согласованность данных ФБО между ФБО |
| FPT_TRC.1 | Согласованность дублируемых данных ФБО |
| FPT_TST.1 | Тестирование ФБО |
| FRU_ FLT.2 | Ограниченная отказоустойчивость |
| FRU_PRS.1 | Ограниченный приоритет обслуживания |
| FRU_RSA.1 | Максимальные квоты |
| FTA_SSL.1 | Блокирование сеанса, инициированное ФБО |
| FTA_SSL.2 | Блокирование, инициированное пользователем |
| FTA_TSE.1 | Открытие сеанса с ОО |
| FTP_TRP.1 | Доверенный маршрут |
| VDS_VMM.1 (EXT) | Отделение домена виртуальных машин |

#### 5.1.1.1 Аудит безопасности (FAU)

**FAU_GEN.1 Генерация данных аудита**

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

а) запуск и завершение выполнения функций аудита;

б) [события, приведенные во втором столбце таблицы 5.2].

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

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

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в 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_SAR.1 | Чтение информации из записей аудита | |
| FAU_SAR.2 | Неуспешные попытки читать информацию из записей аудита | |
| FAU_SEL.1 | Все модификации конфигурации аудита, происходящие во время сбора данных аудита | |
| FAU_STG.3 | Формирование предупреждения после превышения порога заполнения журнала аудита | |
| FAU_STG.4 | Предотвращение регистрации событий или выполнение останова ОО при переполнении журнала аудита | |
| FDP_ACF.1 | Все запросы на выполнение операций на объекте, на который распространяется политика дискреционного управления | Идентификатор объекта |

| Компонент | Событие | Детализация |
|---|---|---|
| | доступом | |
| FDP_IFF.1 | Все решения по запросам на информационные потоки | |
| FIA_AFL.1 | Блокирование учетной записи в результате превышения 10 неуспешных попыток доступа к ОО | |
| 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 (EXT) | Успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта) | |
| FMT_MOF.1 | Все модификации режимов функционирования функций, указанных в компоненте FMT_MOF.1 | |
| FMT_MSA.1 (1) | Все модификации значений атрибутов безопасности, перечисленных в элементе FDP_ACF.1.1 компонента FDP_ACF.1 | |
| FMT_MSA.1 (2) | Все модификации атрибутов управления доступом, ассоциированных с именованным объектом | |
| FMT_MSA.3 (1) | Модификации настройки по умолчанию ограничительных правил политики дискреционного управления доступом. Все модификации начальных значений атрибутов безопасности, используемых в политике дискреционного управления доступом | |

| Компонент | Событие | Детализация |
|---|---|---|
| FMT_MTD.1 | Все модификации значений данных ФБО, указанных в таблице 5.3 | |
| FMT_MTD.2 | Модификация порового значения количества неуспешных попыток аутентификации | |
| FMT_REV.1 (1) | Все попытки отменить атрибуты безопасности, ассоциированные с пользователями ОО | |
| FMT_REV.1 (2) | Все попытки отменить атрибуты безопасности, ассоциированные с объектами | |
| FMT_SAE.1 | Назначение срока действия для аутентификационных данных. Блокирование ассоциированной с пользователем учетной записи | |
| FMT_SMR.1 | Модификация группы пользователей – исполнителей роли пользователя ОО и администратора ОО. Каждое использование прав, предоставляемых ролью пользователя ОО и администратора ОО | Роль |
| FPT_AMT.1 | Выполнение тестирования аппаратной среды и результаты тестирования | |
| FPT_RCV.1 | Сбой и прерывание обслуживания | Тип сбоя и прерывания |
| FPT_SSP.1 | Проведение репликации | |
| FPT_STM.1 | Изменения внутреннего представления времени | |
| FPT_TDC.1 | Применение групповой политики | |
| FPT_TRC.1 | Проведение репликации после восстановления соединения | |
| FPT_TST.1 | Выполнение и результаты самотестирования ФБО | |
| FRU_PRS.1 | Изменение приоритета процесса | |

| Компонент | Событие | Детализация |
|---|---|---|
| FRU_RSA.1 | Квотирование томов файловой системы и объектов службы каталогов | |
| 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.1 «Выбор момента идентификации».

**FAU_SAR.1 Просмотр аудита**

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

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** воспринимать содержащуюся в них информацию.

Зависимости: FAU_GEN.1 «Генерация данных аудита».

**FAU_SAR.2 Ограниченный просмотр аудита**

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

Зависимости: FAU_SAR.1 «Просмотр аудита».

**FAU_SAR.3 Выборочный просмотр аудита**

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

[

следующих атрибутах:

а) идентификатор пользователя;

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

в) источник события;

г) категория события;

д) код события;

е) временной интервал совершения события;

ж) идентификатор учетной записи компьютера

].

Зависимости: FAU_SAR.1 «Просмотр аудита».

**FAU_SEL.1 Избирательный аудит**

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

а) *идентификатор пользователя*;

[

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

в) источник события;

г) категория события;

д) код события;

е) временной интервал совершения события;

ж) идентификатор учетной записи компьютера

].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 «Управление данными ФБО».

**FAU_STG.1 Защищенное хранение журнала аудита**

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

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

Зависимости: FAU_GEN.1 «Генерация данных аудита».

**FAU_STG.3 Действия в случае возможной потери данных аудита**

FAU_STG.3.1 ФБО должны выполнить [формирование предупреждения администратору ОО], если журнал аудита превышает [определенный администратором ОО размер].

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

**FAU_STG.4 Предотвращение потери данных аудита**

FAU_STG.4.1 ФБО должны *предотвращать события, подвергающиеся аудиту, исключая предпринимаемые уполномоченным* ***администратором ОО***, **или** [выполнить останов ОО] при переполнении журнала аудита.

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

**5.1.1.2 Защита данных пользователя (FDP)**

**FDP_ACC.1 Ограниченное управление доступом**

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

[

а) субъектов – процессов, действующих от имени пользователей;

б) именованных объектов – рабочий стол (Desktop), событие (Event), пара событий (Event pair), порт завершения I/O (I/O Completion Port), задание (Job), ключ реестра (Key), 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) операций между субъектами и объектами – обзор папок, выполнение файлов, содержание папки, чтение данных, чтение атрибутов, чтение дополнительных атрибутов, создание файлов, запись данных, создание папок, дозапись данных, запись атрибутов, запись дополнительных атрибутов, удаление, чтение разрешений, смена разрешений, смена владельца, удаление подпапок и файлов

].

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

**FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности**

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

[

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

б) следующих, ассоциированных с объектом, атрибутах управления доступом:

[

– владелец объекта;

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

  – тип (разрешение или запрет);

  – идентификатор пользователя или группы;

  – право доступа к объекту;

]

].

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

[

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

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

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

в) список DACL отсутствует;

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

].

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

[

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

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

].

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

[

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

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

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

].

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

**FDP_IFC.1 Ограниченное управление информационными потоками**

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

[

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

б) информации – входящего 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 политики фильтрации информации не заданы].

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

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

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

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

FMT_MSA.3 «Инициализация статических атрибутов».

**FDP_RIP.1 Ограниченная защита остаточной информации**

FDP_RIP.1.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания **памяти** при *<u>освобождении **памяти**</u>* [процессами].

Зависимости: отсутствуют.

**5.1.1.3 Идентификация и аутентификация (FIA)**

**FIA_AFL.1 Обработка отказов аутентификации**

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [установленное администратором ОО число (не более 10)] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

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

[

а) сделать невозможным доступ субъекта доступа к ОО, осуществив блокировку регистрационной записи на 30 минут;

б) по истечении 30 минут осуществить сброс счетчика неуспешных попыток аутентификации

].

Зависимости: FIA_UAU.1 «Выбор момента аутентификации».

**FIA_ATD.1 Определение атрибутов пользователя**

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

[

а) идентификатор пользователя;

б) принадлежность к группе;

в) привилегии;

г) права доступа к ОО

].

Зависимости: отсутствуют.

**FIA_SOS.1 Верификация секретов**

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

[

а) минимальная длина – 8 символов;

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

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

– прописные буквы английского алфавита от A до Z;

– строчные буквы английского алфавита от a до z;

– десятичные цифры от 0 до 9;

– символы, не принадлежащие алфавитно-цифровому набору;

].

Зависимости: отсутствуют.

**FIA_UAU.2 Аутентификация до любых действий пользователя**

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

Зависимости: FIA_UID.1 «Выбор момента идентификации».

**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.1 «Выбор момента аутентификации».

**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 (EXT) Связывание пользователь-субъект**

FIA_USB.1.1 (EXT) 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 (EXT) 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 (EXT) ФБО должны устанавливать следующие правила, определяющие возможность изменения атрибутов безопасности пользователя, ассоциированных с субъектами, действующими от имени пользователя:

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

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

#### 5.1.1.4 Управление безопасностью (FMT)

**FMT_MOF.1 Управление режимом выполнения функций безопасности**

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

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3 – Управляемые функции и характеристики безопасности

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

| Компонент | Функции ФБО | Операция | Управляемая характеристика |
|---|---|---|---|
| | | добавление | управление функциями из числа ФБО |
| FMT_MSA.1 (1) | управление безопасностью | удаление, модификация, добавление | состав групп безопасности, имеющих привилегии на модификацию атрибутов безопасности, перечисленных в элементе FDP_ACF.1.1 компонента FDP_ACF.1 |
| FMT_MSA.1 (3) | управление безопасностью | удаление, модификация, добавление | состав групп безопасности, имеющих привилегии на модификацию атрибутов безопасности, перечисленных в элементе FDP_IFF.1.1 компонента FDP_IFF.1 |
| FMT_MSA.1 (4) | управление безопасностью | удаление, модификация, добавление | состав групп безопасности, имеющих привилегии на модификацию атрибутов безопасности для правил, перечисленных в элементе FDP_IFF.1.2 компонента FDP_IFF.1 |
| FMT_MSA.3 (2) | управление безопасностью | удаление, модификация, добавление | состав групп безопасности, имеющих привилегии на определение начальных значений |
| FMT_MTD.1 (1) | управление безопасностью | удаление, модификация, добавление | состав групп безопасности, имеющих привилегии на модификацию данных ФБО, указанных в таблице 5.4 |
| FMT_MTD.1 (2) | управление безопасностью | удаление, модификация, добавление | список пользователей, уполномоченных на модификацию собственных аутентификационных данных |
| FMT_MTD.2 | управление | удаление, | состав групп безопасности, |

| Компонент | Функции ФБО | Операция | Управляемая характеристика |
|---|---|---|---|
| | безопасностью | модификация, добавление | имеющих привилегии на модификацию порогового значения количества неуспешных попыток аутентификации |
| FMT_REV.1 (1) | управление безопасностью | удаление, модификация, добавление | состав групп безопасности, имеющих привилегии на отмену атрибутов безопасности, ассоциированных с пользователями ОО |
| FMT_SAE.1 | управление безопасностью | удаление, модификация, добавление | состав групп безопасности, имеющих привилегии на назначение срока действия аутентификационных данных |
| FMT_SMR.1 | управление безопасностью | удаление, модификация, добавление | состав пользователей ОО, являющихся участниками ролей администратор ОО и пользователь ОО |
| FPT_AMT.1 | защита ФБО | установление, модификация | условиями, при которых происходит тестирование аппаратного обеспечения ОО |
| FPT_ITT.1 | защита ФБО | осуществление настройки | механизм, используемый для обеспечения защиты данных ФБО при репликации состояния безопасности |
| FPT_RCV.1 | защита ФБО | установление, модификация | список доступа к средствам восстановления в режиме аварийной поддержки |
| FPT_TST.1 | защита ФБО | установление, модификация | условия, при которых происходит самотестирование ФБО |
| FRU_PRS.1 | использование ресурсов | установление, модификация | приоритеты субъектов |
| FRU_RSA.1 | использование | установление, | квоты на томах файловой |

| Компонент | Функции ФБО | Операция | Управляемая характеристика |
|---|---|---|---|
| | ресурсов | модификация | системы и объектах службы каталогов |
| FTA_SSL.1 | блокирование сеанса | установление, модификация | интервал времени бездействия пользователя ОО и администратора ОО |
| FTA_TSE.1 | доступ к ОО | установление, модификация | идентификатор пользователя; имя компьютера; срок действия аутентификационных данных; время доступа |

**FMT_MSA.1 (1) Управление атрибутами безопасности**

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность *модифицировать* атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [уполномоченному администратору ОО].

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

**FMT_MSA.1 (2) Управление атрибутами безопасности**

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

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

**FMT_MSA.1 (3) 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 [уполномоченному администратору ОО].

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

**FMT_MSA.1 (4) Управление атрибутами безопасности**

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

Зависимости: [FDP_ACC.1 «Ограниченное управление доступом» или FDP_IFC.1 «Ограниченное управление информационными потоками»] 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 владельцем объекта] определять альтернативные начальные значения для отмены значений по умолчанию при создании **объекта**.

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

**FMT_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** [уполномоченному администратору ОО] определять альтернативные начальные значения для отмены значений по умолчанию при создании **правила фильтрации**.

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

**FMT_MTD.1 (1) Управление данными ФБО**

FMT_MTD.1.1 ФБО должны **предоставлять** возможность [*выполнения операций, указанных во втором столбце таблицы 5.4*], над данными, [указанными в третьем столбце таблицы 5.4], только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.4 – Управляемые данные ФБО

| Компонент | Операция | Данные ФБО |
|---|---|---|
| FAU_GEN.1 | удаление, очистка, создание | журнал аудита |
| FAU_STG.3 | установление, модификация | размер журнала аудита |
| FIA_ATD.1 | установление, модификация | атрибуты безопасности пользователя |
| FIA_UAU.2 | установление, модификация | аутентификационные данные (пароль) |
| FIA_UID.2 | установление, модификация | идентификатор пользователя |
| FIA_USB.1 (EXT) | переопределение | заданные по умолчанию атрибуты безопасности пользователя |
| FPT_STM.1 | модификация | представление времени |

**FMT_MTD.1 (2) Управление данными ФБО**

FMT_MTD.1.1 ФБО должны **предоставлять** возможность *модификации* [собственных аутентификационных данных] только [уполномоченному пользователю ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

**FMT_MTD.2 Управление ограничениями данных ФБО**

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

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

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

**FMT_REV.1 (1) Отмена**

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

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

[

а) отмена полномочий у пользователей ОО и администраторов ОО на доступ к объектам должна вступать в силу при следующем сеансе работы пользователя ОО и администратора ОО;

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

].

Зависимости: FMT_SMR.1 «Роли безопасности».

**FMT_REV.1 (2) Отмена**

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

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

[

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

].

Зависимости: FMT_SMR.1 «Роли безопасности».

**FMT_SAE.1 Ограниченная по времени авторизация**

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

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

Зависимости: FMT_SMR.1 «Роли безопасности»,
FPT_STM.1 «Надежные метки времени».

**FMT_SMR.1 Роли безопасности**

FMT_SMR.1.1 ФБО должны поддерживать следующие роли**:**

[

а) администратор ОО;

б) пользователь ОО

].

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

Зависимости: FIA_UID.1 «Выбор момента идентификации».

#### 5.1.1.5 Защита ФБО (FPT)

**FPT_AMT.1 Тестирование абстрактной машины**

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

Зависимости: отсутствуют.

**FPT_FLS.1 Сбой с сохранением безопасного состояния**

FPT_FLS.1 ФБО должны сохранять безопасное состояние при следующих типах сбоев:

[

а) отключение электропитания на активном узле ОО;

б) потеря взаимодействия между узлами ОО;

в) возникновение аппаратного сбоя на узле ОО

].

Зависимости: ADV_SPM.1 «Неформальная модель политики безопасности ОО».

**FPT_ITT.1 Базовая защита внутренней передачи данных ФБО**

FPT_ITT.1.1 ФБО должны защитить свои данные от *раскрытия и модификации* при **репликации состояния безопасности, проводимой** между **разными компьютерами с установленными экземплярами ОО (в случае совместного обеспечения безопасности)**.

Зависимости: отсутствуют.

**FPT_RCV.1 Ручное восстановление**

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

Зависимости: FPT_TST.1 «Тестирование ФБО»,
AGD_ADM.1 «Руководство администратора»,
ADV_SPM.1 «Неформальная модель политики безопасности ОО».

**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_SSP.1 Одностороннее надежное подтверждение**

FPT_SSP.1.1 ФБО должны подтвердить после запроса **от компьютеров с установленными экземплярами ОО (в случае совместного обеспечения безопасности)** получение немодифицированных данных ФБО при **репликации состояния безопасности**.

Зависимости: FPT_ITT.1 «Базовая защита внутренней передачи данных ФБО».

**FPT_STM.1 Надежные метки времени**

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

Зависимости: отсутствуют.

**FPT_TDC.1 Базовая согласованность данных ФБО между ФБО**

FPT_TDC.1.1 ФБО должны обеспечить способность согласованно интерпретировать **следующие данные ФБО:**

[

а) идентификационную информацию;

б) аутентификационную информацию;

в) информацию авторизации;

г) настройки безопасности;

д) управляющие и служебные данные, необходимые для безопасного функционирования ОО, серверных и клиентских ОС

],

совместно используемые ФБО и **управляемыми (со стороны ОО) клиентскими и серверными ОС**.

FPT_TDC.1.2 ФБО должны использовать [правила интерпретации не предусмотрены] при интерпретации данных ФБО, полученных от **управляемых клиентских и серверных ОС**.

Зависимости: отсутствуют.

**FPT_TRC.1 Согласованность дублируемых данных ФБО**

FPT_TRC.1.1 ФБО должны обеспечить согласованность данных ФБО при **репликации состояния безопасности, проводимой между ФБО и компьютерами с установленными экземплярами ОО (в случае совместного обеспечения безопасности)**.

FPT_TRC.1.2 Когда **компьютеры с установленными экземплярами ОО**, содержащие дублируемые данные ФБО, **недоступны**, ФБО должны обеспечить согласованность дублируемых данных ФБО после восстановления соединения перед обработкой любых запросов ко [всем функциям безопасности].

Зависимости: FPT_ITT.1 «Базовая защита внутренней передачи данных ФБО».

**FPT_TST.1 Тестирование ФБО**

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

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

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

Зависимости: FPT_AMT.1 «Тестирование абстрактной машины».

### 5.1.1.6 Использование ресурсов (FRU)

**FRU_ FLT.2 Ограниченная отказоустойчивость**

FRU_FLT.2.1 ФБО должны обеспечить выполнение **всех возможностей ОО**, когда происходят следующие сбои:

[

а) отключение электропитания на активном узле ОО;

б) потеря взаимодействия между узлами ОО;

в) возникновение аппаратного сбоя на узле ОО

].

Зависимости: FPT_FLS.1 «Сбой с сохранением безопасного состояния».

**FRU_PRS.1 Ограниченный приоритет обслуживания**

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

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

Зависимости: отсутствуют.

**FRU_RSA.1 Максимальные квоты**

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

Зависимости: отсутствуют.

### 5.1.1.7 Доступ к ОО (FTA)

**FTA_SSL.1 Блокирование сеанса, инициированное ФБО**

FTA_SSL.1.1 ФБО должны блокировать интерактивный сеанс после [истечения интервала времени бездействия пользователя ОО или администратора ОО], для чего предпринимаются следующие действия:

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

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

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

Зависимости: FIA_UAU.1 «Выбор момента аутентификации».

**FTA_SSL.2 Блокирование, инициированное пользователем**

FTA_SSL.2.1 ФБО должны допускать инициированное пользователем **ОО или администратором ОО** блокирование своего собственного интерактивного сеанса, для чего предпринимаются следующие действия:

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

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

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

Зависимости: FIA_UAU. 1 «Выбор момента аутентификации».

**FTA_TSE.1 Открытие сеанса с ОО**

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса, основываясь на **следующем:**

[

а) идентификатор пользователя;

б) имя компьютера;

в) срок действия аутентификационных данных;

г) время доступа

].

Зависимости: отсутствуют.

#### 5.1.1.8 Доверенный маршрут/канал (FTP)

**FTP_TRP.1 Доверенный маршрут**

FTP_TRP.1.1 ФБО должны предоставлять маршрут связи между собой и *локальным* пользователем **ОО или администратором ОО**, 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 **ОО или администраторам ОО*** инициировать связь через доверенный маршрут.

FTP_TRP.1.3 ФБО должны требовать использования доверенного маршрута для *начальной аутентификации пользователя **ОО или администратора ОО** [и разблокирования сеанса].*

Зависимости: отсутствуют.

#### 5.1.1.9 Отделение домена виртуальных машин (VDS)

**VDS_VMM.1 (EXT) Отделение домена виртуальных машин**

VDS_VMM.1.1 (EXT) ФБО должны поддерживать домен безопасности для функционирования каждой виртуальной машины, который должен защищать виртуальную машину от вмешательства и искажения недоверенными субъектами или субъектами, находящимися вне области действия виртуальной машины.

VDS_VMM.1.2 (EXT) ФБО должны реализовывать разделение между доменами безопасности виртуальных машин в ОДФ.

Зависимости: отсутствуют.

### 5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 ОК и образуют ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности ОО) (см. таблицу 5.5).

Таблица 5.5 – Требования доверия к безопасности ОО

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

#### 5.1.2.1 Управление конфигурацией (ACM)

**ACM_CAP.1 Номера версий**

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

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

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

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

#### 5.1.2.2 Поставка и эксплуатация (ADO)

**ADO_IGS.1 Процедуры установки, генерации и запуска**

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

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

#### 5.1.2.3 Разработка (ADV)

**ADV_FSP.1 Неформальная функциональная спецификация**

Элементы действий разработчика

ADV_FSP.1.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

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

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

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

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

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

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

**ADV_RCR.1 Неформальная демонстрация соответствия**

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

### 5.1.2.4 Руководства (AGD)

**AGD_ADM.1 Руководство администратора**

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

#### 5.1.2.5 Тестирование (ATE)

**ATE_IND.1 Независимое тестирование на соответствие**

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

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

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

#### 5.1.2.6 Оценка уязвимостей (AVA)

**AVA_SOF.1 Оценка стойкости функции безопасности ОО**

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

Элементы действий оценщика

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

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

## 5.2 Требования безопасности для ИТ-среды

У объекта оценки нет ИТ-среды.

# 6 Краткая спецификация ОО

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

## 6.1 Функции безопасности ОО

ОО реализует следующие функции безопасности:

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

### 6.1.1 Функции безопасности «Аудит безопасности»

Аудит безопасности − это одно из важнейших средств поддержания безопасности системы. В рамках общей стратегии безопасности необходимо определить уровень аудита, который подходит для среды. Аудит должен определять как успешные, так и безуспешные атаки, представляющие собой угрозу сети или направленные на ресурсы, которые были признаны ценными при оценке рисков.

Функции безопасности ОО «Аудит безопасности» обеспечивают:

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

#### 6.1.1.1 Сбор данных аудита

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

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

Справочный монитор безопасности SRM, выполняемый в режиме ядра, и подсистема LSASS, функционирующая в пользовательском режиме, осуществляют взаимодействие друг с другом с использованием механизма локального вызова процедур LPC (Local Procedure Call). При инициализации системы монитор безопасности SRM создает коммуникационный порт *SeRmCommandPort*, к которому подключается процесс LSASS. В свою очередь, процесс LSASS при запуске также создает LPC-порт *SeLsaCommandPort*, подключение к которому осуществляет монитор безопасности SRM. В результате указанных действий формируются закрытые коммуникационные порты (см. рисунок 6.1). Монитор SRM создает раздел общей памяти для передачи сообщений длиннее 256 байт и передает его описатель при запросе на соединение. После соединения монитора безопасности SRM и подсистемы LSASS на этапе инициализации системы они больше не прослушивают свои порты. Поэтому никакой пользовательский процесс не сможет подключиться к одному из указанных портов.

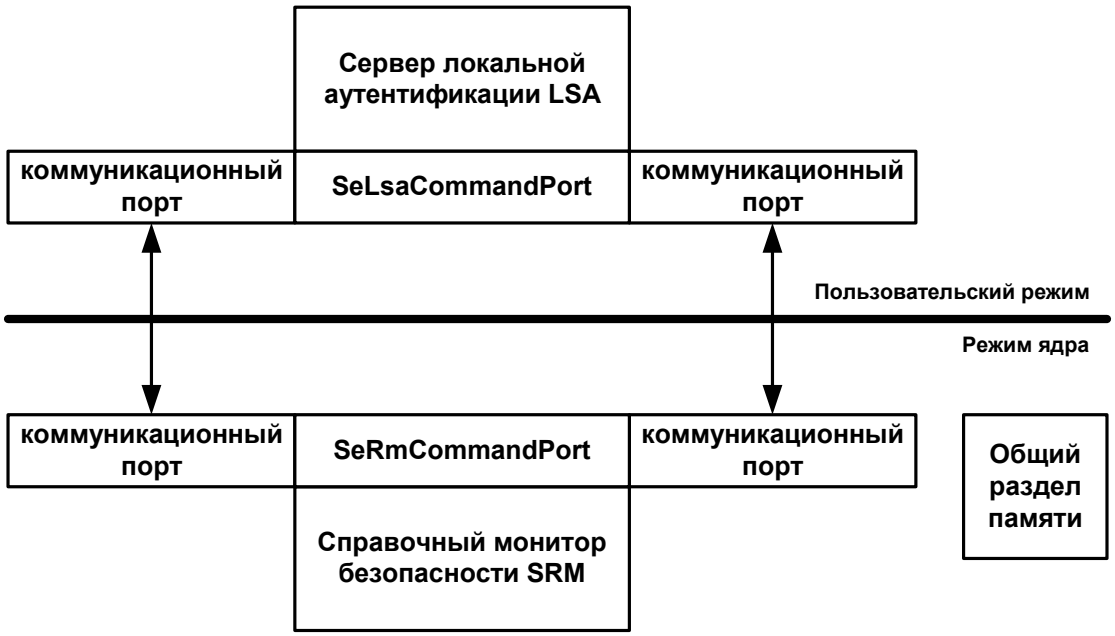



Рисунок 6.1.

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

Подсистема LSASS, помимо передачи монитору безопасности SRM текущей конфигурации политики аудита, также отвечает за прием записей аудита, генерируемых на основе событий аудита от монитора безопасности SRM, их редактирование и передачу регистратору событий Event Logger. Эти записи передает именно подсистема LSASS (а не монитор SRM), так как она добавляет в них сопутствующую дополнительную информацию, например информацию, нужную для более полной идентификации процесса, по отношению к которому проводится аудит.

Монитор безопасности SRM осуществляет передачу записей аудита подсистеме LSASS через свое LPC-соединение. После этого регистратор событий Event Logger заносит записи аудита в журнал безопасности. В дополнение к записям аудита,

передаваемым монитором SRM, подсистема LSASS тоже генерирует записи аудита, которые она пересылает непосредственно регистратору событий Event Logger (см. рисунок 6.2).

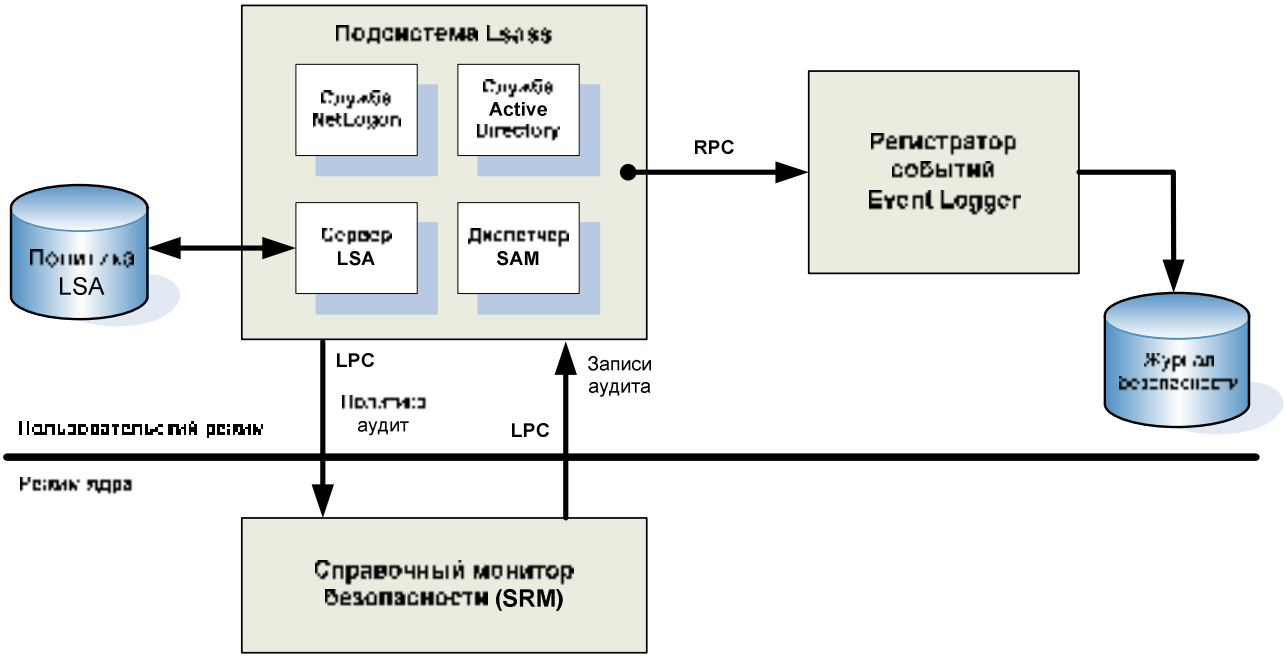



Рисунок 6.2.

Записи аудита, подлежащие пересылке, помещаются в очередь процесса LSASS по мере получения – они не передаются пакетами. Пересылка этих записей осуществляется одним из двух способов. Если запись аудита невелика (меньше максимального размера LPC-сообщения), она посылается как LPC-сообщение. Записи аудита копируются из адресного пространства монитора безопасности SRM в адресное пространство процесса LSASS. Если запись аудита велика, монитор безопасности SRM делает ее доступной процессу LSASS через разделяемую память и передает LSASS указатель на нее, используя для этого LPC-сообщение.

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

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

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

Таблица 6.1 – Сведения записей аудита.

| Сведения | Описание |
|---|---|
| Дата | Дата, соответствующая событию. |
| Время | Время, когда произошло данное событие. |
| Пользователь | Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала аудита событий безопасности содержит оба кода. |
| Компьютер | Имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, если только просмотр событий не выполняется с другого компьютера. |
| Код события | Число, определяющее конкретный тип события. В первой строке описания обычно содержится название типа события. Код события и имя источника записи могут использоваться для устранения неполадок. |
| Источник | Программа, инициирующая событие. Это может быть как имя программы, так и название компонента системы или приложения, например, название драйвера. В случае журнала аудита событий безопасности источник события определяется как «Security». |
| Тип | Уровень важности событий. В журнале аудита событий безопасности записи событий могут быть двух типов – «Аудит успехов» и «Аудит отказов». Событие безопасности относится к типу «Аудит успехов», если |

| Сведения | Описание |
|---|---|
| | соответствует успешно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае успешного входа пользователя в систему в журнал аудита событий безопасности заносится событие аудита типа «Аудит успехов». Событие безопасности относится к типу «Аудит отказов», если соответствует отказу в доступе. Например, в случае неудачной попытке доступа пользователя к сетевому диску в журналаудита событий безопасности заносится событие аудита типа «Аудит отказов». |
| Категория | Категория события в зависимости от источника события. Для аудита событий безопасности категория соответствует одному из типов событий, для которых в политике аудита может быть включен аудит успехов или отказов. |

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

Таблица 6.2 – Политики аудита.

| № п/п | Политика аудита | Описание политики |
|---|---|---|
| **1.** | Аудит системных событий. | Политика системных событий записывает в журнал аудита событий безопасности указанные события, например перезапуск или выключение компьютера. |
| **2.** | Аудит входов в систему. | В журнал аудита событий безопасности могут заноситься входы через сеть или с помощью служб. |
| **3.** | Аудит доступа к объектам. | Политика доступа к объектам записывает в журнал аудита событий безопасности события при попытке доступа пользователя к какому-либо ресурсу (например, к принтеру или совместно используемой папке). |
| **4.** | Аудит привилегированного | Привилегированное использование является |

| № п/п | Политика аудита | Описание политики |
|---|---|---|
| | использования. | параметром безопасности и может включать применение пользователем своих прав, изменение системного времени и тому подобное. В журнал аудита событий безопасности могут записываться успешные или неудачные попытки. |
| **5.** | Аудит отслеживания процессов. | Для каждой программы или процесса, запускаемого пользователем, могут записываться события. Эта информация может быть очень подробной и требует значительного объема ресурсов. |
| **6.** | Аудит изменения политик. | При каждой попытке изменения политики (права пользователя, политики аудита учетных записей, политики доверительных отношений) записывается событие. |
| **7.** | Аудит управления учетными записями. | При изменении учетных записей в журнал аудита событий безопасности могут записываться события, доступные для последующего просмотра. |
| **8.** | Аудит доступа к службам каталогов. | При каждой попытке доступа пользователя к объекту Active Directory, который имеет свой собственный системный список контроля доступа (System Access Control List – SACL), в журнале фиксируется соответствующее событие. |
| **9.** | Аудит событий входной регистрации учетных записей. | При каждой попытке входа пользователя может записываться успешное или неудачное событие. Неудачные попытки входа могут указывать на неудачи при входе для неизвестных пользовательских учетных записей, нарушения ограничения времени, просроченные учетные записи, недостаточные права для локального входа пользователя, просроченные пароли учетных записей и заблокированные учетные записи. |

Политики аудита могут быть включены или отключены с помощью либо политики локальной системы, либо политики безопасности контроллера домена, либо объектов групповых политик.

Общие категории подразделяются на подкатегории, для каждой из которых можно указать значение NO Auditing (Не выполнять аудит), Success (Успех), Failure (Неудача) или Success and Failure (Успех и неудача). Эти категории позволяют администраторам более точно указывать события, подверженные аудиту.

Соответствие категорий и политик описано в таблице 6-3.

Таблица 6.3 – Соответствие политик аудита и категорий аудита.

| № п/п | Политика аудита | Категория аудита |
|---|---|---|
| **1.** | Аудит системных событий. | System (Система). |
| **2.** | Аудит входов в систему. | Logon/Logoff (Входы и выходы). |
| **3.** | Аудит доступа к объектам. | Object Access (Доступ к объектам). |
| **4.** | Аудит привилегированного использования. | Privilege Use (Привилегированное использование) |
| **5.** | Аудит отслеживания процессов. | Detailed Tracking (Детальное отслеживание). |
| **6.** | Аудит изменения политик. | Policy Change (Изменение политик). |
| **7.** | Аудит управления учетными записями. | Account Management (Управление учетными записями). |
| **8.** | Аудит доступа к службам каталогов. | DS Access (Доступ к DS). |
| **9.** | Аудит событий входной регистрации учетных записей. | Account Logon (Входная регистрация учетных записей). |

Имеется более 50 категорий, значения которых можно устанавливать по отдельности. Категории и подкатегории политики аудита приведены в таблице 6.4.

Таблица 6.4 – Подкатегории аудита.

| № п/п | Категория аудита | Подкатегория аудита |
|---|---|---|
| **1.** | System (Система). | Security State Change (Изменение состояния безопасности).<br>Security System Extension (Системное расширение безопасности).<br>System Integrity (Целостность системы).<br>IPSec Driver (Драйвер IPSec).<br>Other System Events (Другие системные события). |
| **2.** | Logon/Logoff (Входы и выходы). | Logon (Вход).<br>Logoff (Выход).<br>Account Lockout (Блокировка учетных записей).<br>IPSec Main Mode (Основной режим IPSec).<br>IPSec Quick Mode (Быстрый режим IPSec).<br>IPSec Extended (Расширенный режим IPSec).<br>Special Logon (Специальный выход).<br>Network Policy Server (Сервер сетевых политик).<br>Other Logon/Logoff Events (Другие события входов и выходов). |
| **3.** | Object Access (Доступ к объектам). | File System (Файловая система).<br>Registry (Системный реестр).<br>Kernel Object (Объект ядра).<br>SAM.<br>Certification Services (Служба сертификатов).<br>Application Generated (Сгенерированное приложение).<br>Handle Manipulation (Ручные действия).<br>File Share (Общие файловые ресурсы).<br>Filtering Platform Packet Drop (Отбрасывание пакетов фильтрующей платформы).<br>Filtering Platform Connection (Подключение фильтрующей платформы).<br>Other Object Access Events (Другие события доступа в систему). |
| **4.** | Privilege Use (Привилегированное | Sensitive Privilege Use (Использование опасных полномочий). |

| № п/п | Категория аудита | Подкатегория аудита |
|---|---|---|
| | использование) | Non Sensitive Privilege Use (Использование безопасных полномочий).<br>Other Privilege Use Events (Другие события использования полномочий). |
| **5.** | Detailed Tracking (Детальное отслеживание). | Process Creation (Создание процесса).<br>Process Termination (Завершение процесса).<br>DPAPI Activity (Активность DPAPI).<br>RPC Events (События RPC). |
| **6.** | Policy Change (Изменение политик). | Audit Policy Change (Аудит изменения политик).<br>Authentication Policy Change (Изменение политик аутентификации).<br>Authorization Policy Change (Изменение политик авторизации).<br>MPSSVC Rule-Level Policy Change (Изменение политик уровня правил MPSSVC).<br>Filtering Platform Policy Change (Изменение политик фильтрующей платформы).<br>Other Policy Change Events (Другие события изменения политик). |
| **7.** | Account Management (Управление учетными записями). | User Account Management (Управление учетными записями пользователей).<br>Computer Account Management (Управление учетными записями компьютеров).<br>Security Group Management (Управление группами безопасности).<br>Distribution Group Management (Управление группами распространения).<br>Application Group Management (Управление группами применения).<br>Other Account Management Events (Другие события управления учетными записями). |
| **8.** | DS Access (Доступ к DS). | Directory Service Access (Доступ к службе каталогов).<br>Directory Service Change (Изменения в службе каталогов). |

| № п/п | Категория аудита | Подкатегория аудита |
|---|---|---|
| | | Directory Service Replication (Репликация службы каталогов).<br>Detailed Directory Service Replication (Детализированная репликация службы каталогов). |
| **9.** | Account Logon (Входная регистрация учетных записей). | Kerberos Service Ticket Operation (Операции с билетами службы Kerberos).<br>Credential Validation (Проверка полномочий).<br>Kerberos Authentication Service (Служба аутентификации Kerberos).<br>Other Account Logon Events (Другие события входной регистрация учетных записей). |

ФБО способны отслеживать и регистрировать события безопасности, соответствующие определенным категориям событий аудита, описание которых представлено выше.

**6.1.1.2 Просмотр журналов аудита**

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

**6.1.1.3 Защита журнала аудита от переполнения**

Объект оценки предотвращает потерю данных аудита событий безопасности посредством управления регистрацией и очередью событий аудита. Исходя из настроек ОО, данные аудита добавляются в журнал аудита событий безопасности до тех пор, пока он не станет полным. ОО обеспечивает защиту данных аудита от потери, используя возможность генерировать событие аудита в случае, если размер журнала аудита событий безопасности достигнет установленного для него порогового значения. Кроме того, уполномоченный администратор может сконфигурировать ОО на запрет затирания

данных аудита (т.е. очистка журнала аудита событий безопасности будет осуществляться вручную) или немедленное завершение работы в случае переполнения журнала аудита событий безопасности. При такой конфигурации, в случае завершения работы ОО в результате переполнения журнала аудита событий безопасности, повторную регистрацию в ОО может выполнить только уполномоченный администратор. В случае заполнения журнала аудита событий безопасности на дисплей администратора выводится сообщение, указывающее, что произошло переполнение журнала аудита событий безопасности аудита.

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

ФБО обеспечивают сбор информации о событиях безопасности посредством справочного монитора безопасности SRM и подсистемы LSASS. Оба компонента подсистемы безопасности ОО поддерживают собственные очереди событий аудита. Монитор безопасности SRM помещает записи аудита во внутреннюю очередь для последующей их передачи подсистеме LSASS, которая со своей стороны поддерживает вторую очередь, содержащую в себе данные аудита, переданные монитором безопасности SRM и другими службами. Обе очереди событий аудита отслеживают возможную потерю данных аудита. Монитор безопасности SRM определяет верхнюю и нижнюю метку для собственной очереди событий аудита, что позволяет отследить момент ее заполнения. Подсистема LSASS также поддерживает метки для собственной очереди событий аудита с целью определения момента ее заполнения.

Потеря данных аудита может произойти в случае, если очереди подсистемы LSASS и монитора безопасности SRM достигнут установленных для них значений верхних меток, либо в случае, когда размер файла журнала аудита событий безопасности достигнет своего предела, который не может превышать 4 Гб.

#### 6.1.1.4 Ограничение доступа к журналу аудита

Для просмотра содержимого журнал аудита событий безопасности пользователь должен быть определен в роли администратора, т.е. являться участником соответствующих групп безопасности, обладающих административными полномочиями, либо иметь привилегию «Управление аудитом или журналом безопасности», дающей пользователю полномочия на просмотр журнала регистрации событий безопасности. Журнал аудита событий безопасности является системным ресурсом, создаваемым на этапе установки системы. ОО не располагает интерфейсами, позволяющими создавать, удалять или изменять журнал аудита событий безопасности. Подсистема локальной аутентификации LSASS является единственной службой, обеспечивающей запись событий в журнал аудита событий безопасности.

**Сопоставление с ФТБ**

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

- FAU_GEN.1 – ОО обеспечивает генерацию данных аудита для всех категорий и подкатегорий событий, представленных в таблицах 6.3 и 6.4, а также событий, связанных с функционированием брандмауэра сетевых подключений. Для каждого события аудита ФБО регистрируют дату, время, идентификатор пользователя или его имя, идентификатор события, источник, тип, категорию и подкатегорию события;
- FAU_GEN.2 – ФБО обеспечивают ассоциирование каждого события, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события;
- FAU_SAR.1 – инструментальные средства просмотра событий предоставляют администратору ОО возможность просмотра данных аудита в удобочитаемом формате;
- FAU_SAR.2 – ФБО предоставляют доступ к чтению записей аудита только уполномоченным администраторам ОО;
- FAU_SAR.3 – инструментальные средства просмотра событий аудита предоставляют возможность выполнения поиска и сортировки данных аудита

по идентификатору пользователя, типу результата события (успех и/или отказ), источнику события, категории события, коду события, временному интервалу совершения события, идентификатору учетной записи компьютера;

- FAU_SEL.1 – ФБО предоставляют возможность включать события, потенциально подвергаемые аудиту, в совокупность событий, подвергающихся аудиту;
- FAU_STG.1 – ФБО защищают хранимые записи аудита от несанкционированного изменения и предотвращают их модификацию;
- FAU_STG.3 – ОО может быть настроен на генерацию события аудита (предупреждение о превышении размера) в случае превышения данными аудита установленного для журнала аудита событий безопасности размера;
- FAU_STG.4 – ОО может быть настроен на предотвращение генерации событий аудита или выполнение аварийного останова в случае переполнения журнала аудита событий безопасности.

### 6.1.2 Функции безопасности «Защита данных пользователя»

К предоставляемым ОО механизмам обеспечения защиты данных пользователя относятся:

- дискреционное (избирательное) 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 и в контексте их безопасности, т.е. в рамках определенных для пользователей полномочий. В таблице 6.5 представлен перечень объектов данных пользователя, на которые распространяется политика дискреционного управления доступом, устанавливаемая для ОО.

Таблица 6.5 – Перечень объектов, на которые распространяется политика дискреционного управления доступом.

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

| № п/п | Именованные объекты | Описание |
|---|---|---|
| **8.** | Мутант (Mutant) | Объект, создаваемый для механизма межпроцессного взаимодействия (известный как Mutex в win32 интерфейсе). |
| **9.** | Порт LPC (LPC port) | Объект механизма вызова локальных процедур. |
| **10.** | Почтовый ящик (Mail slot) | Объект ввода/вывода, предоставляющий механизм ненадежного одностороннего широковещания. |
| **11.** | Именованный канал (Named Pipe) | Объект ввода/вывода, используемый для обеспечения надежной двусторонней связи 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. |
| **15.** | Каталог AD (Active Directory) | Представление общих ресурсов, определяемых и поддерживаемых службой каталогов Active Directory. |
| **16.** | Процесс (Process) | Совокупность потоков, выполняющихся в едином контексте и имеющих общее виртуальное адресное пространство и управляющую информацию. |
| **17.** | Секция (Section) | Область памяти. |
| **18.** | Семафор (Semaphore) | Счетчик, действующий как шлюз к ресурсам. Позволяет указывать максимальное число потоков, которым разрешен доступ к защищенным этим объектом ресурсам. |
| **19.** | Символьная ссылка (Symbolic Link) | Механизм косвенной ссылки на имя объекта. |
| **20.** | Запланированная задача (Scheduled Task) | Программа, которая выполняется в определенное время или когда происходит определенное событие. |
| **21.** | Поток (Thread) | Представляет исполнительную часть процесса. Все потоки в пользовательском режиме ассоциированы с процессами. |
| **22.** | Таймер (Timer) | Механизм уведомления потока об истечении фиксированного периода времени. |

| № п/п | Именованные объекты | Описание |
|---|---|---|
| **23.** | Маркер доступа (Access Token) | Представляет контекст безопасности процессов или потоков. |
| **24.** | Том (Volume) | Один или несколько разделов, отформатированных для использования файловой системой. |
| **25.** | Объект «Window-Station» | Объект, содержащий буфер обмена и группу объектов «рабочий стол». |
| **26.** | Отладка (Debug) | Набор ресурсов, используемых для процессов отладки. |
| **27.** | Порт Связи Фильтра (Filter Connection Port) | Представляет драйвер мини-фильтра. |
| **28.** | Порт Коммуникации Фильтра (Filter Communication Port) | Представляет порт для связи с драйвером мини-фильтра. |

**Идентификаторы безопасности (Security Identifiers)**

Для обеспечения уникальной идентификации субъектов доступа, выполняющих в системе различные действия, ОО использует не символьные имена (которые не являются уникальными), а идентификаторы безопасности SID. Идентификаторы безопасности SID представляют структуру данных переменной длины, определяющей учетные записи пользователей, локальных и доменных групп безопасности, компьютеров и доменов. Внутренние процессы ОО обращаются к учетным записям по их идентификаторам безопасности SID, а не по именам пользователей, групп или компьютеров.

Идентификатор безопасности SID представляет собой числовое значение переменной длины, формируемое из номера версии структуры SID, 48-битного кода агента идентификатора, переменного количества 32-битных кодов субагентов и относительных идентификаторов RID (relative identifiers). Код агента идентификатора (identifier authority value) определяет агента, выдавшего идентификатор безопасности SID. Таким агентом обычно является локальная система или контроллер домена, функционирующий под управлением ОО. Коды субагентов идентифицируют попечителей, уполномоченных агентом, который выдал идентификатор безопасности SID, а относительные идентификаторы RID используются в качестве средства создания

уникальных идентификаторов безопасности SID на основе общего базового идентификатора безопасности (common-based SID). В текстовой форме каждый идентификатор безопасности SID начинается с префикса S, за которым следуют группы чисел, разделяемые дефисами (S-1-5-<domain SID>-<RID>).

Идентификатор безопасности SID назначается компьютеру при установке ОО. Далее ОО присваивает идентификаторы SID локальным или доменным учетным записям.

Идентификатор безопасности SID каждой учетной записи формируется на основе идентификатора безопасности SID компьютера с добавлением относительных идентификаторов RID. Относительные идентификаторы RID пользовательской учетной записи начинается с 1000 и увеличивается на 1 для каждого нового пользователя или группы безопасности. Аналогичным образом ОО формирует идентификаторы безопасности SID для участников домена. Новые учетные записи пользователей или групп домена получают идентификаторы безопасности SID, формируемые на основе идентификатора безопасности SID домена с добавлением относительного идентификатора RID (который также начинается с 1000 и увеличивается на 1 для каждого нового пользователя или группы).

Ряд предопределенных учетных записей пользователей обладает идентификаторами безопасности SID, состоящими из идентификатора безопасности SID компьютера или домена и предопределенного идентификатора RID. Так, относительный идентификатор RID встроенной учетной записи администратора равен 500, а идентификатор RID гостевой учетной записи – 501.

Встроенным локальным и доменным группам безопасности ОО также назначает ряд предопределенных идентификаторов безопасности SID.

**Атрибуты субъектов дискреционного управления доступом**

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

В процессе регистрации в ОО служба WinLogon создает начальный маркер доступа, представляющий пользователя, который входит в ОО, и сопоставляет его с

процессом оболочки – пользовательским интерфейсом. Далее все программы, запускаемые пользователем, наследуют копию этого маркера.

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

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

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

Устанавливаемый по умолчанию дискреционный список управления доступом DACL представляет собой атрибуты безопасности, применяемые ОО в отношении

создаваемых субъектом доступа (процессом или потоком) объектов. Включая в маркеры доступа указанную информацию, ОО упрощает процессам и потокам создание объектов со стандартными атрибутами безопасности, так как в этом случае им не требуется запрашивать информацию о списках DACL при создании каждого объекта доступа.

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

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

Механизм имперсонации применяется в основном в «клиент-серверных» архитектурах. Например, в случае, когда субъект обращается к защищаемым сетевым активам, расположенным на сервере. Получив запрос на доступ, сервер должен убедиться в наличии у субъекта разрешений на выполнение над активами запрошенных операций. Так, если пользователь на удаленной машине пытается удалить файл с сетевого диска NTFS, сервер, поддерживающий указанный сетевой объект, должен проверить, имеет ли пользователь право удалить данный файл. При этом на этапе проверки прав доступа субъекта будет задействован механизм имперсонации.

Механизм имперсонации позволяет серверу уведомить справочный монитор безопасности SRM о временном заимствовании контекста безопасности субъекта, запрашивающего ресурс. После этого сервер может обращаться к ресурсам от имени субъекта доступа, а справочный монитор безопасности SRM – проводить проверку его прав доступа.

Сервер имперсонирует субъекта лишь в пределах потока, выдавшего запрос на имперсонацию. Управляющие структуры данных потока содержат необязательный элемент для маркера доступа. Однако основной маркер потока, отражающий его реальные права, всегда доступен через управляющие структуры процесса.

За поддержку возможности имперсонации в ОО отвечает несколько механизмов. Если сервер взаимодействует с клиентом (субъектом) через именованный канал (Named Pipe), он может вызвать функцию *ImpersonateNamedPipeClient* и тем самым сообщить монитору безопасности SRM о том, что ему нужно подменить собой пользователя на другом конце канала. Если сервер взаимодействует с клиентом (субъектом) через механизмы динамического обмена данными DDE (Dynamic Data Exchange) или удаленного вызова процедур RPC, то запрос на имперсонацию осуществляется через функции *DdeImpersonateClient* или *RpcImpersonateClient*. Поток может создать имперсонированный маркер доступа просто как копию маркера своего процесса, вызвав функцию *ImpersonateSelf*. Для блокировки каких-либо идентификаторов безопасности SID или привилегий поток впоследствии может изменить полученный имперсонированный маркер доступа. После того как серверный поток завершает выполнение своей задачи, его исполнение осуществляется в собственном контексте безопасности.

Объект оценки обеспечивает защиту при использовании механизмов имперсонации, не позволяя серверам подменять клиентов (субъектов доступа) без их контроля. Клиентский процесс может ограничить уровень имперсонации серверным процессом, сообщив при соединении с ним требуемый SQOS (Security Quality of Service). Процесс может указывать следующие флаги:

- SECURITY_ANONYMOUS;
- SECURITY_IDENTIFICATION;
- SECURITY_IMPERSO-NATION;
- SECURITY_DELEGATION.

Данные флаги определяют соответствующие уровни имперсонации. Каждый уровень позволяет серверному процессу выполнять различный набор операций относительно контекста безопасности субъекта доступа:

- *Anonymous* – самый ограниченный уровень имперсонации; серверный процесс может имперсонировать субъекта, однако имперсонированный маркер доступа

не содержит какой-либо информации, позволяющей идентифицировать субъекта;

- *Identify* – серверный процесс может получать идентификатор безопасности SID и привилегии субъекта, но не обладает правом его имперсонации;
- *Impersonate* – серверный процесс может идентифицировать и имперсонировать клиента (выступать от его имени) только в локальной системе; если серверный процесс функционирует на удаленном компьютере, он может имперсонировать клиента только в случае его доступа к активам, содержащимся на данном компьютере;
- *Delegate* – наименее ограниченный уровень имперсонации. Позволяет серверному процессу имперсонировать субъект доступа как в локальных, так и в удаленных системах.

Если клиентский процесс явно не устанавливает уровень имперсонации, ОО по умолчанию выбирает уровень Impersonate.

Остальные поля маркера служат для информационных целей. Поле источника маркера содержит сведения (в текстовой форме) о создателе маркера. Оно позволяет различать такие источники, как диспетчер сеансов ОО или RPC-сервер. Идентификатор маркера представляет собой локально уникальный идентификатор LUID (locally unique identifier), который справочный монитор безопасности SRM присваивает маркеру доступа при его создании. Атрибут политики аудита используется для аудита «на пользователя». Атрибут происхождения маркера доступа определяет возможные пути формирования маркера доступа: в результате регистрации пользователя с явным указанием его идентификационных и аутентификационных данных, либо аутентификации через сеть.

**Ограниченные маркеры**

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

- удалить некоторые элементы из таблицы привилегий, предоставленных субъекту доступа;

– пометить идентификаторы безопасности SID, содержащиеся в маркере, атрибутом проверки только на запрет (deny-only);
– пометить идентификаторы безопасности SID-идентификаторы, содержащиеся в маркере, как ограниченные (restricted SID).

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

**Атрибуты объектов дискреционного управления доступом**

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

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

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

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

Существуют два типа строк управления доступом ACE:

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

Записи ACE типа «разрешенный объект» и «запрещенный объект» имеют поле глобально уникального идентификатора GUID (Globally Unique Identifier), которое сообщает, что запись ACE применима только к определенным объектам или подобъектам Active Directory (с GUID-идентификаторами). GUID-идентификатор – это гарантированно уникальный 128-битный идентификатор объекта.

За счет аккумуляции прав доступа, определяемых отдельными записями ACE, ОО формируется действительный набор прав доступа, предоставляемых дискреционным списком управления доступом DACL. Если дескриптор безопасности объекта не содержит списка DACL (нулевой DACL – Null DACL), любой пользователь имеет полный доступ к объекту. Если список DACL пуст, т.е. в нем нет записей ACE, доступ к указанному объекту будет запрещен для всех субъектов доступа.

Каждая из записей ACE, используемых в списках DACL, также имеет набор атрибутов, контролирующих и определяющих характеристики ACE, связанные с наследованием. Наследование представляет собой процесс распространения записей ACE из списка управления доступом ACL родительского объекта в список ACL дочернего объекта. В ОО наследование записей ACE дочерними объектами может осуществляться в следующих случаях:

- при создании нового дочернего объекта;
- при изменении списка DACL родительского объекта;
- при изменении списка SACL родительского объекта.

Атрибуты наследования определяют 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. Описание поддерживаемых ОО атрибутов наследования записей ACE представлено в таблице 6.6.

Таблица 6.6 – Описание атрибутов наследования записей ACE.

| № п/п | Атрибут наследования | Назначение |
|---|---|---|
| **1.** | CONTAINER_INHERIT_ACE | Дочерние объекты, являющиеся контейнерами для других объектов (например, каталоги в пространстве имен файловой системы), наследуют записи ACE с установленным атрибутом CONTAINER_INHERIT_ACE в качестве действительных (effective) записей ACE. В случае наследования записи ACE с указанным атрибутом ОО сбрасывает атрибут INHERIT_ ONLY_ACE. |
| **2.** | INHERIT_ONLY_ACE | Указывает, что запись ACE является только наследуемой ACE (inherit-only ACE). Данная запись ACE не учитывается на этапе проверки прав доступа к объекту. Если данный атрибут не определен, запись ACE распознается ОО в качестве действительной ACE (effective ACE), т.е. записи ACE, учитываемой при проверке прав доступа к объекту. |
| **3.** | INHERITED_ACE | Указывает, что данная запись управления |

| № п/п | Атрибут наследования | Назначение |
|---|---|---|
| | | доступом ACE унаследована из списка DACL родительского объекта. ОО устанавливает данный атрибут наследования при передаче дочернему объекту наследуемой записи ACE. |
| **4.** | NO_PROPAGATE_INHERIT_ ACE | Если дочерний объект наследует запись ACE, где установлен данный атрибут наследования, то ОО автоматически сбрасывает атрибуты OBJECT_ INHERIT_ACE и CONTAINER_INHERIT_ACE в унаследованной записи ACE, что предотвращает ее наследование последующими поколениями объектов. |
| **5.** | OBJECT_INHERIT_ACE | Дочерние объекты, не являющиеся контейнерами для других объектов, наследуют записи ACE с установленным атрибутом OBJECT_INHERIT_ ACE в качестве действительных (effective) записей ACE. В случае наследования записи ACE с указанным атрибутом ОО сбрасывает атрибут INHERIT_ ONLY_ACE. |

Элементами системного списка управления доступом являются записи управления доступом ACE двух типов:

– запись ACE системного аудита (system-audit ACE);
– запись ACE объекта системного аудита (system-audit object ACE).

Данные записи ACE определяют, какие операции, выполняемые над объектами доступа конкретными пользователями или группами, подлежат аудиту. Записи ACE объекта системного аудита поддерживаются только для объектов службы каталога Active Directory и содержат поле глобально уникального идентификатора GUID, указывающее типы объектов или подобъектов Active Directory, к которым применимы данные записи ACE. При нулевом списке назначений аудита SACL (SACL = null) аудит доступа к объекту не ведется.

Атрибуты наследования, определяемые в списках DACL для записей ACE, применимы также к записям ACE системного аудита и объектов системного аудита.

**Механизм проверки прав доступа**

Модель защиты объекта оценки требует, чтобы субъект доступа заранее − еще до доступа к объекту – указывал, какие операции он собирается выполнять над данным объектом. Система проверяет тип доступа, запрошенный субъектом (потоком), и, если такой доступ ему разрешен, он получает описатель, позволяющий ему выполнять операции над объектом. Когда субъект (поток) создает объект или открывает описатель существующего объекта, он должен указать маску запрашиваемых прав доступа (desired access rights), определяющих действия, которые субъект доступа намеревается выполнить в отношении указанного объекта.

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

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

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

в созданном им описателе объекта, т.е. осуществляется ассоциация маски назначенного доступа с каждым открытым описателем.

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

Для объектов в режиме ядра описатели представлены в таблице описателей (handle table) режима ядра. Для каждого процесса определена своя таблица описателей, каждая строка которой идентифицирует открытый объект и права доступа, назначенные для данного объекта. В пользовательском режиме механизм использования описателей аналогичен режиму ядра, т.е. с помощью таблицы описателей определяется расположение необходимого объекта и ассоциированная с ним маска назначенного доступа. В обоих случаях, и для объектов пользовательского режима, и для объектов режима ядра, контроль доступа реализуется монитором безопасности SRM.

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

**Алгоритм реализации политики дискреционного управления доступом**

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

Представленный ниже алгоритм дает краткое описание механизма принятия решения о разрешении доступа к объекту данных пользователя. Для того чтобы предоставить субъекту доступ к объекту, необходимо выполнить проверку прав его доступа, указанных в маске запрашиваемого доступа. Проверка прав выполняется по шагам в порядке следования записей управления доступом ACE до первого запрета на какую-либо операцию или до явного разрешения всех запрошенных операций. В случае

если все строки просмотрены, но осталось хотя бы одно право, не разрешенное явно, доступ будет запрещен.

1. **Наличие дискреционного списка управления доступом**

В случае отсутствия списка DACL (DACL = Null) объект доступа является незащищенным.

2. **Проверка привилегий**

Проверка привилегии SeTakeOwnershipPrivilege. Если маркер доступа запрашивающего субъекта содержит привилегию SeTakeOwnershipPrivilege, дающую право на изменение дескриптора безопасности объекта в части смены его владельца, ОО предоставляет субъекту право на доступ «запись владельца» (WRITE_OWNER) до анализа списка DACL.

3. **Проверка владельца объекта (Owner)**

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

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

4. **Проверка содержимого дискреционного списка управления доступом**

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

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

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

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

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

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

В отношении объектов каталога Active Directory формирование маски предоставленных прав доступа осуществляется на основе следующих правил:

- если тип записи ACE является ACCESS_ALLOWED_OBJECT_ACE 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;
- если тип записи ACE является ACCESS_DENIED_OBJECT_ACE 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 типа доступа задан явный запрет через запись ACE, тогда дальнейшая проверка прав доступа будет прекращена. Если достигнут конец списка DACL и некоторые из запрошенных прав доступа предоставлены не были, доступ к объекту запрещается.

После анализа всех записей ACE списка DACL рассчитанная маска предоставленных прав доступа возвращается вызывающему субъекту как максимальные права доступа. Эта маска отражает полный набор прав доступа, которые можно успешно запрашивать при открытии данного объекта.

**Обеспечение защиты через устанавливаемые по умолчанию права доступа**

Объект оценки обеспечивает 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), то ОО формирует список DACL на его основе. Если объект находится в объекте-контейнере (например, именованное событие в каталоге BaseNamedSecurity пространства имен диспетчера объектов), ОО объединяет в дискреционный список управления доступом DACL все наследуемые от родительского объекта-контейнера записи ACE, но только в том случае, если в дескрипторе безопасности не установлен флаг SE_DACL_PROTECTED, запрещающий наследование записей ACE;
- если вызывающим субъектом доступа в запросе на создание объекта дескриптор безопасности представлен не был, то список DACL формируется на основе списка DACL родительского объекта, но только если представленные в нем записи ACE имеют соответствующие атрибуты наследования, указывающие, что область их применения охватывает все дочерние по отношению к данному объекту-контейнеру объекты;
- если дескриптор безопасности не определен и объект не наследует какие-либо записи ACE от родительского объекта, ОО извлекает из маркера доступа вызывающего субъекта устанавливаемый по умолчанию дискреционный список управления доступом DACL и применяет его к новому объекту;
- если дескриптор безопасности явно не указан запрашивающим субъектом доступа и не существует ни наследуемых от родительского объекта записей ACE, ни устанавливаемого по умолчанию списка DACL, ОО создает объект без DACL (DACL = Null), что открывает полный доступ к нему любым пользователям и группам. Данное правило аналогично предшествующему в случае, если в маркере доступа содержится нулевой список DACL, устанавливаемый по умолчанию для создаваемых объектов доступа.

Правила, используемые ОО при назначении списка SACL новому объекту, аналогичны правилам присвоения списка DACL со следующими ограничениями:

- наследуемые записи ACE системного аудита не передаются объектам в том случае, если в дескрипторе безопасности объекта установлен флаг SE_SACL_PROTECTED, запрещающий наследование записей ACE;
- если записи ACE системного аудита не определены и отсутствует список SACL, наследуемый от родительского объекта, то список назначений аудита SACL объекту доступа не присваивается.

При применении к контейнеру нового дескриптора безопасности, содержащего наследуемые записи ACE, ОО автоматически передает их в дескрипторы безопасности дочерних объектов. При этом список DACL дескриптора безопасности объекта не включает наследуемые записи ACE, если установлен флаг SE_DACL_PROTECTED, указывающий, что список DACL не может быть модифицирован наследуемыми от родительского объекта записями ACL. Аналогичное ограничение действует в отношении списков SACL – список назначений аудита SACL дескриптора безопасности объекта не может быть модифицирован наследуемыми от родительского объекта записями ACL, если установлен флаг SE_SACL_PROTECTED.

При управлении списками ACL в отношении объектов Active Directory дополнительно учитываются следующие аспекты:

- если наследуемая запись ACE удаляется из списка DACL родительского объекта, все копии этой записи ACE автоматически удаляются из всех дочерних объектов;
- если из списка DACL дочернего объекта удалены все записи ACE, у дочернего объекта остается нулевой список DACL.

В соответствии с порядком слияния наследуемых от родительского объекта записей ACE с дескриптором безопасности дочернего объекта любые записи ACE, явно указанные в списках управления доступом ACL данного объекта, следует до записей ACE, унаследованных объектом. ОО использует следующие правила передачи наследуемых записей ACE:

- если для дочернего объекта список DACL явно не определен и объект наследует записи ACE родительского объекта, то его список DACL будет содержать только унаследованные записи ACE;
- если дочерний объект содержит нулевой список DACL и наследует записи ACE родительского объекта, то его список DACL также будет содержать только унаследованные записи ACE.

#### 6.1.2.2 Фильтрация информации

ФБО обеспечивают защиту компьютера, непосредственно подключенного к сети, или компьютеров и устройств, подключенных к компьютеру, через который осуществляется общий доступ к вычислительным сетям, от сетевых атак различных типов.

ФБО обеспечивают проверку допустимости каждой попытки передачи/получения данных в процессе организации информационного обмена с внутренней или внешней вычислительными сетями. Поддерживая таблицу состояния активных соединений (stateful inspection), ФБО позволяют отслеживать все характеристики передаваемого трафика и проверять исходный адрес и адрес назначения в каждом обрабатываемом сообщении и используют полученную информацию, чтобы определить, какие сетевые пакеты разрешается получать ОО. ФБО автоматически разрешают все исходящие соединения, независимо от программ и контекста безопасности, в котором они функционируют.

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

Помимо этого, в процессе регулирования обмена данными учитываются дополнительные параметры (списки исключений и ограничения), определяющие

поведение ФБО и задаваемые администратором ОО исходя из среды функционирования ОО и выполняемых им задач. Передача/получение сетевых пакетов ОО в/из вычислительной сети разрешается только при условии успешного завершения всех проверок.

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

– блокирует подключение;
– разрешает подключение.

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

При задании списка исключения для программ администратор ОО определяет перечень программ, которым разрешается получение незапрашиваемых входящих запросов по любому порту, которые они пытаются открыть. Автоматическое открытие и закрытие требуемых портов осуществляется независимо от контекста безопасности функционирующего в ОО приложения. При этом приложение, включенное в список исключений для программ, может открывать только необходимые для его правильного функционирования порты и только на то время, на которое оно их задействует.

В случае когда определен список исключений для портов, ФБО разрешают непредусмотренные запросы на подключение к персональному компьютеру для конкретной программы или службы через разрешенный порт. Таким образом, ФБО предоставляют программам и службам возможность взаимодействовать через вычислительную сеть без ограничений и ущерба для их функциональности.

Объект оценки поддерживает следующие функции:

– **включен** – ФБО блокирует все внешние запросы к компьютеру, кроме запросов программ и служб, определяемых с использованием политики исключения;
– **выключен** – данный режим функционирования используется в случае, если защита компьютера осуществляется с использованием брандмауэра сторонних производителей.

#### 6.1.2.3 Защита остаточной информации

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

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

Основными элементами управления памятью являются (см. рисунок 6.3):

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

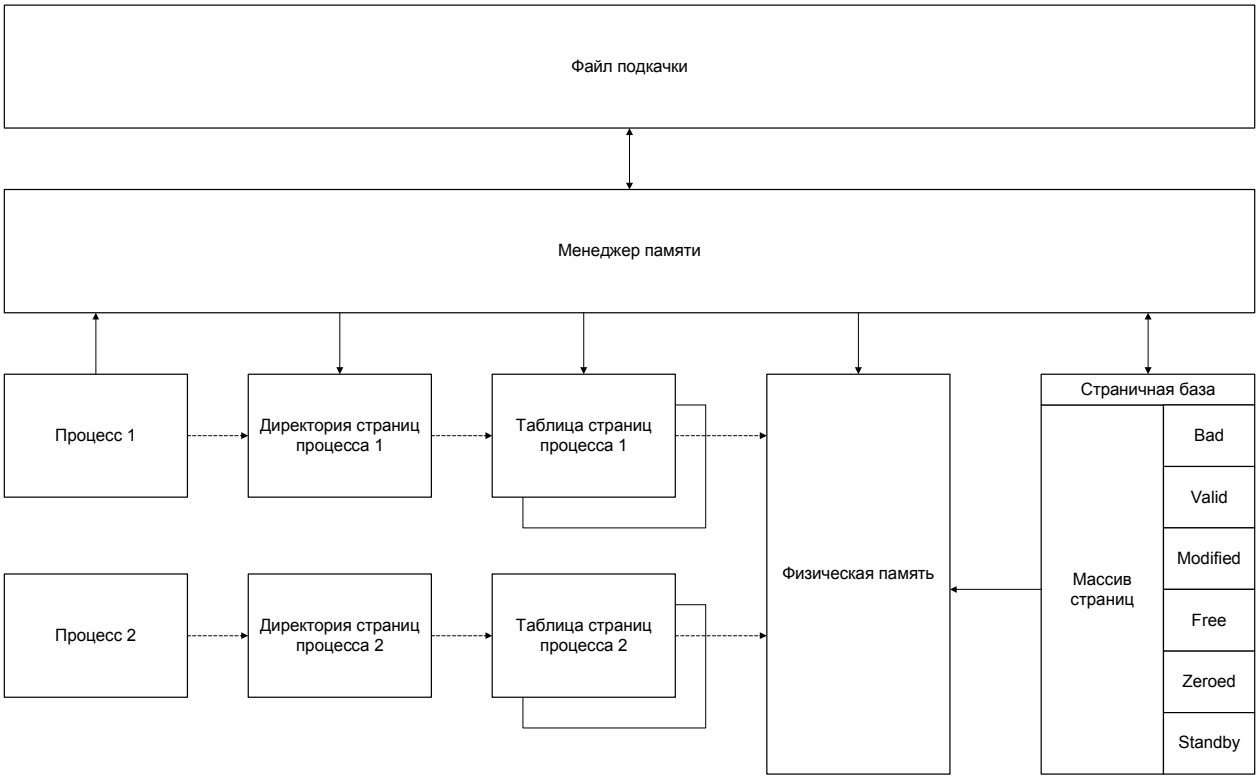



Рисунок 6.3 – Структура управления памятью ОО.

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

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

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

Диспетчер памяти ОО является отдельным системным процессом, отвечающим за:

- поддержание, модификацию и переключение контекстов страниц процессов;

– обработку запросов на актуализацию страниц физической памяти и страничного файла;
– обработку запросов процессов на выделение и освобождение памяти.

В своей работе диспетчер памяти использует страничную базу для хранения информации о состоянии страниц физической памяти.

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

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

Единственным процессом, модифицирующим страничную базу, является диспетчер памяти ОО. Модификация страничной базы включает изменение флагов состояния страниц и списков индексов в ответ на соответствующие события в системе. Граф переходов состояния страниц приведен на рисунке 6.4. При изменении состояния страницы происходит не только изменение ее флагов, но и модификация соответствующих списков индексов.

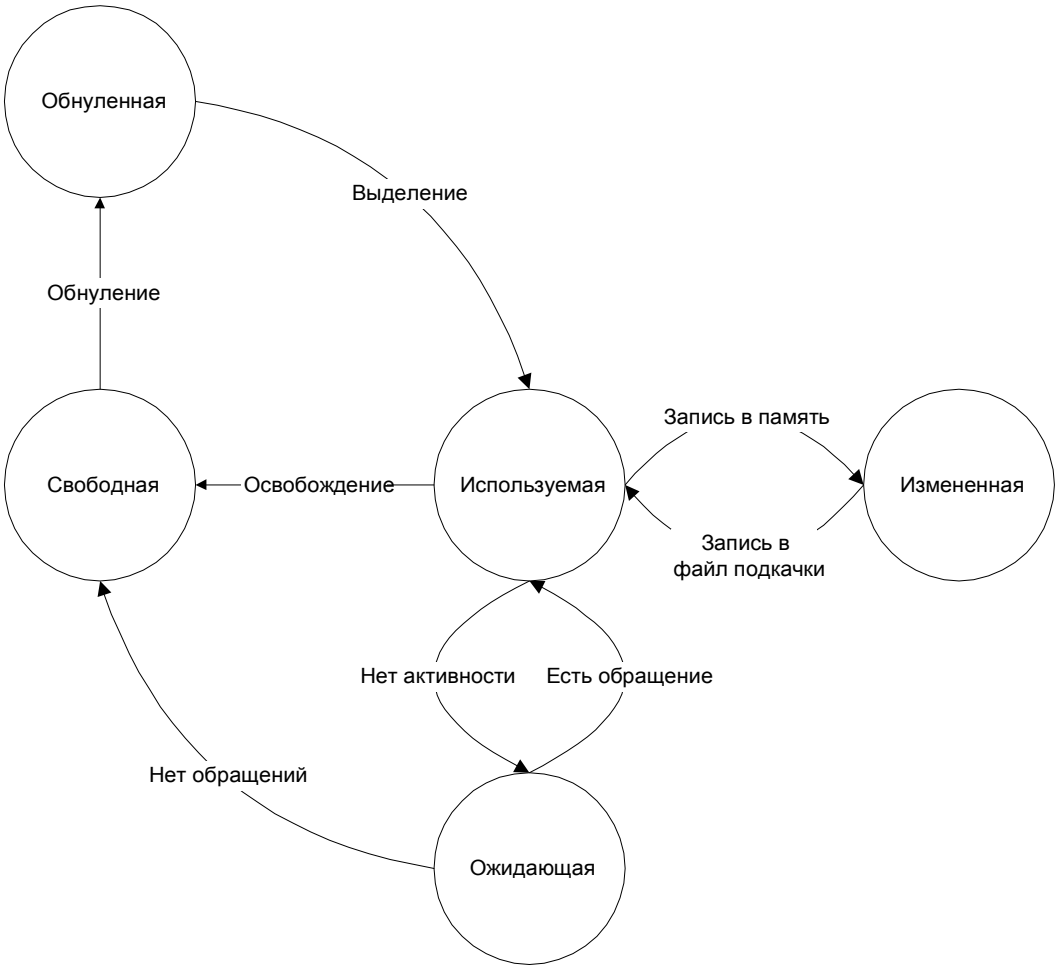



Рисунок 6.4 – Граф переходов состояний страниц памяти, управляемой ОО.

Переходы между состояниями страницы осуществляются при следующих условиях:

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

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

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

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

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

**Сопоставление с ФТБ**

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

– FDP_ACC.1 – в ОО реализован механизм дискреционного управления доступом для субъектов – процессов, действующих от имени пользователей, именованных объектов – рабочий стол (Desktop), событие (Event), пара событий (Event pair), порт завершения I/O (I/O Completion Port), задание (Job), ключ реестра (Key), 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», объект службы каталогов (Active Directory objects) и всех операций между субъектами и объектами;

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

### 6.1.3 Функции безопасности «Идентификация и аутентификация»

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

#### 6.1.3.1 Типы доступа к ОО

Объект оценки поддерживает следующие типы доступа пользователя к ОО:

– интерактивный (Interactive) – локальный доступ пользователя к ОО;
– сетевой (Network) – доступ к ОО через сеть;

- доступ в качестве службы (Batch) – регистрация пользователем процесса в качестве службы;
- доступ в качестве пакетного задания (Service) – доступ пользователя к ОО с помощью средств обработки пакетных заданий;
- разблокировка (Unlock) – тип доступа, имеющий место при разблокировании пользователем рабочей станции;
- «по сети открытым текстом» (NetworkCleartext) – доступ пользователя к ОО из сети, при этом пароль пользователя был передан пакету аутентификации (authentication package) в нехэшированной форме. Все встроенные в ОО пакеты аутентификации перед пересылкой учетных данных пользователей по сети осуществляют их хэширование. Учетные данные субъектов доступа не передаются по сети в открытом виде;
- «новые учетные данные» (NewCredentials) – вызывающая программа скопировала свой текущий маркер доступа и задала новые учетные данные для внешних соединений. Новый сеанс (logon sessions) имеет те же учетные данные, но для других сетевых соединений использует иные учетные данные;
- удаленно-интерактивный (Remote Interactive) – пользователь выполнил доступ к ОО удаленно посредством службы терминалов либо удаленного рабочего стола;
- интерактивный с хэшированными учетными данными (CachedInteractive) − пользователь выполнил доступ к ОО с регистрационными данными доменной учетной записи, которые хранились в локальной памяти компьютера. На контроллере домена подлинность регистрационных данных пользователя не осуществлялась.

Интерактивный доступ к ОО предусматривает доступ пользователя к ОО через локальную консоль и предполагает работу пользователя с ОО в интерактивном режиме. Сетевой доступ используется при обращении пользователя к удаленному компьютеру для доступа к его активам. Доступ в качестве пакетного задания предназначен для случаев, когда процессы могут исполняться от имени пользователя без их непосредственного вмешательства, т.е. пользователь получает возможность доступа к ОО с помощью средства обработки пакетных заданий. Доступ в качестве службы используется, когда

участники безопасности имеют возможность осуществлять доступ к ОО как службы для установления контекста безопасности. Локальная системная учетная запись всегда сохраняет право доступа к ОО в качестве службы. Любая служба, запускаемая с правами конкретной учетной записи, должна быть наделена правом доступа в качестве службы. По умолчанию эта привилегия не предоставляется никому.

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

#### 6.1.3.2 Регистрация пользователя в ОО

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

С целью защиты идентификационной и аутентификационной информации при первоначальном интерактивном доступе пользователя в систему, ОО обеспечивает ее передачу через доверенный маршрут. Доверенный маршрут вызывается одновременным нажатием комбинации клавиш SAS (Secure Attention Sequence) – Ctrl+Alt+Del, что всегда фиксируется ФБО, т.е. данное действие не может быть прервано или перехвачено недоверенным процессом ОО.

В процессе регистрации пользователя в ОО задействованы процессы Winlogon, LSASS, один или несколько пакетов аутентификации, а также база данных SAM или каталог Active Directory, в случае если ОО функционирует в домене. Схема взаимодействия между компонентами ОО, участвующими в процессе регистрации, показана на рисунке 6.5.

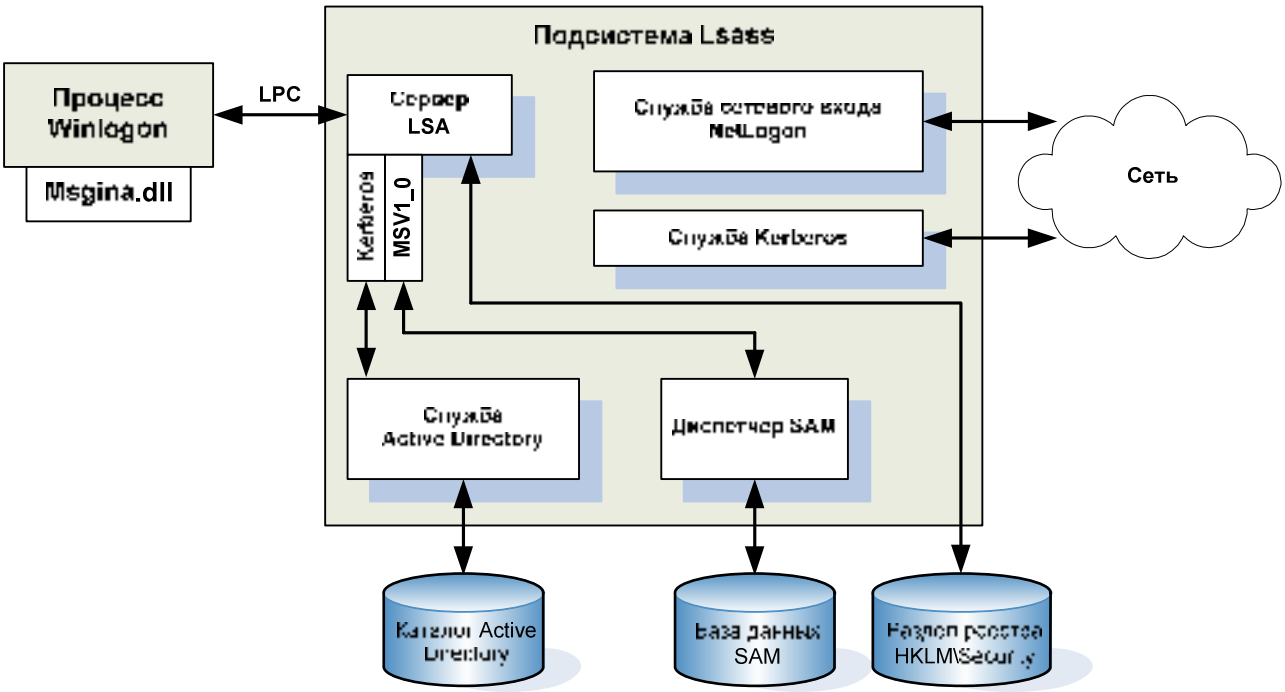



Рисунок 6.5 – Схема взаимодействия между компонентами ОО, участвующими в процессе регистрации пользователя в ОО.

Для получения регистрационных данных от пользователя задействуется служба WinLogon, которая является процессом пользовательского режима, отвечающим за поддержку и управление сеансами интерактивного доступа к ОО. Уведомление о запросе пользователя на регистрацию в ОО служба WinLogon получает при нажатии комбинации клавиш SAS. При этом интерфейс регистрации пользователя в ОО, в частности стандартное диалоговое окно доступа к ОО, обеспечивается DLL-модулем Graphical Identification and Authentication (GINA). Основная задача модуля GINA – сбор идентификационной и аутентификационной информации, вводимой пользователем, и передача ее процессу WinLogon. Служба WinLogon, получив имя и пароль пользователя от модуля GINA, передает его в строго определенном формате серверному процессу локальной аутентификации LSASS, который отвечает за получение от службы WinLogon запросов на аутентификацию и вызов пакетов аутентификации для проверки соответствия введенной пользователем аутентификационной информации той, что хранится в каталоге Active Directory или базе данных SAM.

Модель аутентификации, поддерживаемая в ОО, реализована по модульному принципу на основе пакетов аутентификации (Authentication Packages). Модульность

архитектуры позволяет абстрагировать основные системные процедуры аутентификации от конкретных протоколов и реализации. Пакет аутентификации – основной компонент, реализующий логику проверки параметров пользователя и в конечном итоге принимающий решение об успешной или неуспешной регистрации. Пакет аутентификации представляет собой библиотеку DLL, которая подключается к процессу LSASS при старте ОО. ОО поддерживаются два пакета аутентификации:

- MSV1_0 (\Winnt\System32\Msv1_0.dll) – пакет аутентификации, обеспечивающий интерактивную локальную регистрацию пользователя, регистрацию пользователя в отсутствие контроллера домена и поддержку протокола аутентификации NTLM;
- Kerberos (\Winnt\System32\Kerberos.dll) – пакет аутентификации, реализующий поддержку протокола Kerberos v5 rev.6, являющегося основным протоколом аутентификации, используемым ОО. Обеспечивает интерактивную и неинтерактивную регистрацию пользователей в домене Active Directory.

Для аутентификации пользователей в домене Active Directory ОО по умолчанию используют протокол Kerberos. Это означает, что ОО всегда сначала будет инициировать аутентификацию по этому протоколу. Только при невозможности обнаружить и установить связь со службами Kerberos будет использован протокол NTLM (или же вообще в регистрации будет отказано).

**Интерактивная локальная регистрация пользователя в ОО**

1. Регистрация пользователя в ОО начинается с момента нажатия им комбинации клавиш SAS (Ctrl+Alt+Del) и явного запроса системой у пользователя его регистрационных данных. Для получения информации от пользователя задействуются служба WinLogon и модуль Graphical Identification and Authentication.

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

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

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

5. В противном случае, MSV1_0 переходит к этапу сравнения хэшированного пароля и имени пользователя с теми, которые хранятся в базе данных SAM (в случае интерактивной регистрации с хэшированными учетными данными пакет аутентификации MSV1_0 обращается к хэшированной информации через функции LSASS, отвечающие за сохранение и получение информации из базы данных сервера LSA – раздела реестра HKLM\SECURITY). Если регистрационные данные пользователя совпадают с данными, хранящимися в базе данных SAM, MSV1_0 генерирует LUID-идентификатор сеанса регистрации и создает собственно сеанс регистрации вызовом LSASS. При этом MSV1_0 сопоставляет данный уникальный идентификатор с сеансом и передает данные, необходимые для того, чтобы создать маркер доступа для пользователя.

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

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

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

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

**Регистрации пользователя в домене**

Базовая последовательность действий при использовании пакета аутентификации Kerberos в основном та же, что и в случае с MSV1_0. Однако в большинстве случаев доменная регистрация проходит на рабочих станциях или серверах, входящих в домен (а не на контроллере домена), поэтому пакет аутентификации в процессе проверки подлинности должен взаимодействовать со службой Kerberos на контроллере домена.

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

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

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

Чтобы получить доступ к защищаемым ресурсам клиент посылает службе Ticket Granting Service (TGS) запрос, содержащий полученный билет TGT. Служба Kerberos генерирует и посылает ответ от службы Ticket Granting Service. Он содержит сессионный

билет (session ticket). В данном билете содержатся идентификатор безопасности учетной записи и всех глобальных групп, скопированных службой Kerberos с оригинального билета TGT. На основании этого билета сервер, содержащий защищаемые активы, аутентифицирует пользователя и формирует для него маркер доступа

Главным компонентом службы Kerberos является центр распределения ключей KDC (Key Distribution Center), функционирующий как доменная служба на контроллере домена (ОО). В соответствии со спецификацией Kerberos центр распределения ключей KDC исполняется как единый процесс, обеспечивающий две службы:

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

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

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

Между двумя механизмами аутентификации (по протоколу Kerberos и NTLM) существуют два основных отличия. Первое заключается в том, что запрос NTLM, содержащий имя пользователя и пароль в хэшированном виде, пересылается ФБО на сервер. Сервер сравнивает представленный в хэшированном виде пароль с версией, хранящейся в базе данных. Если пароли совпадают, аутентификация считается успешной. В случае локальной аутентификации пароли не хэшируются и серверу не передаются, пароль сравнивается с хранящимся в локальной базе данных экземпляром. Kerberos, напротив, требует, чтобы запрос на доступ был частично преобразован с помощью хэшированного пароля. Преобразованный запрос пересылается соответствующему контроллеру домена, который в свою очередь ищет хешированный пароль пользователя в своей базе данных. Далее данный пароль используется для обратного преобразования запроса на вход. Если операция обратного преобразования выполнена успешно и запрос на вход содержит соответствующие временные метки (т.е. определен в рамках временного периода, установленного администратором), аутентификация считается успешной.

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

#### 6.1.3.3 База данных атрибутов пользователя

Объект оценки поддерживает базу данных, в которой полностью определены учетные записи пользователей и групп безопасности. При этом хранение доменных

учетных записей пользователей, групп и компьютеров осуществляется в каталоге Active Directory на контролерах домена, а учетных записей пользователей и групп, определенных на локальном компьютере, в базе данных диспетчера учетных записей безопасности SAM (Security Account Manager).

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

- *имя учетной записи* – используется для представления учетной записи в удобочитаемой форме;
- *идентификатор безопасности SID* – идентификатор, используемый для однозначного представления учетной записи пользователя или группы в рамках ОО;
- *пароль* – используется только для учетных записей пользователей. Основная задача заключается в аутентификации учетной записи пользователя при его входе в ОО;
- *принадлежность к группе* – 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 доступ к системе* – право, присвоенное пользователю и определяющее способы его доступа к системе;
- *управляющая информация* – используется, чтобы контролировать дополнительные относящиеся к безопасности параметры учетных записей, такие как время действия учетной записи, факт блокировки, срок действия пароля, история паролей и время последнего изменения пароля;
- *другая информация, не относящаяся к безопасности,* – используется для дополнительного описания учетной записи, например, действительное имя и предназначение учетной записи.

Действительная совокупность всех атрибутов учетных записей пользователей и групп безопасности зависит от роли, исполняемой компьютером. Если ОО функционирует на компьютере, исполняющем роль рядового сервера, в этом случае ОО будет поддерживать собственную базу данных для локальных учетных записей пользователей и

групп, которые будут описаны одной совокупностью атрибутов. В случае функционирования ОО на компьютере, исполняющем роль контроллера домена, совокупность атрибутов описывающих доменные учетные записи пользователей и групп будет значительно расширена.

#### 6.1.3.4 Политики учетных записей

Политики учетных записей определяются взаимодействие учетных записей пользователей с компьютерами или доменами. Управление политиками доменных учетных записей осуществляется централизованно через групповую политику «Default Domain Policy» (Политика домена, используемая по умолчанию), определяемую на уровне домена. Политики учетных записей определяются и управляются уполномоченным администратором. Через политики учетных записей можно задать политику паролей, политику блокировки учетной записи и политику Kerberos.

**Политика паролей**

С использованием политики паролей определяются следующие параметры паролей:

- *максимальный срок действия пароля* – определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем ОО потребует от пользователя заменить его. Значение для данного параметра может быть определено в диапазоне от 1 до 999 дней. Установив число дней равным 0, можно снять всякие ограничения срока действия пароля;
- *минимальная длина пароля* – определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Значение для данного параметра может быть определено в диапазоне от 1 до 14 символов. Установив число символов равным 0 можно отменить использование пароля;
- *минимальный срок действия пароля* – определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Значение для данного параметра может быть определено в диапазоне от 1 до 998 дней. Установив число дней равным 0 можно разрешить немедленное изменение пароля пользователем. Минимальный срок действия пароля должен быть меньше, чем максимальный срок действия

пароля, если только не задан неограниченный срок действия пароле установкой значения 0. Чтобы действие параметра «Требовать неповторяемости паролей» было эффективным, необходимо установить минимальный срок действия пароля, отличный от нуля. Если этого не сделать, пользователь сможет перебрать все свои пароли и дойти до старого пароля, который он предпочитает. По умолчанию при развертывании домена для данного параметра устанавливается значение, равное 1;

- *пароль должен отвечать требованиям сложности* – данное требование определяет, должны ли пароли отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:
  - пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
  - пароль должен состоять не менее чем из восьми символов;
  - в пароле должны присутствовать символы как минимум трех категорий из числа следующих:
    - прописные буквы английского алфавита (от A до Z);
    - строчные буквы английского алфавита (от a до z);
    - десятичные цифры (от 0 до 9);
    - специальные символы (например, !, $, #, %), символы из расширенного набора ASCII, символические или лингвистические знаки.

Требования сложности, контролируемые данным параметром политики, хранятся в файле Passfilt.dll. Проверка соблюдения этих требований выполняется при изменении или создании паролей. По умолчанию данный параметр включен в политику паролей, определяемую на контроллерах домена через групповую политику «Default Domain Policy»;

- *требовать неповторяемость паролей* – определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24. Данная политика позволяет

уполномоченным администраторам повышать уровень безопасности, запрещая все время использовать одни и те же старые пароли. Чтобы добиться эффективной сменяемости паролей, необходимо запретить немедленную замену паролей при настройке параметра «Минимальный срок действия пароля». По умолчанию в политике паролей, определяемой на контроллерах домена через групповую политику «Default Domain Policy», параметру «Требовать неповторяемость паролей» присвоено значение 24;

– *хранить пароли, используя обратимое преобразование* – определяет, использует ли ОО обратимое преобразование для хранения паролей. Использование данного параметра позволяет обеспечить поддержку приложений, использующих протоколы, которым для проверки подлинности необходимо знать пароль пользователя. По умолчанию данный параметр отключен в политике паролей, определяемой на контроллерах домена через групповую политику «Default Domain Policy».

**Политика блокировки учетной записи**

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

– *временной интервал блокировки учетной записи* – определяет число минут, в течение которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Значение для данного параметра может быть определено в диапазоне от 1 до 99 999 минут. Если установить значение 0, учетная запись будет блокирована на все время до тех пор, пока администратор не разблокирует ее явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса. По умолчанию данный параметр не определен;

– *пороговое значение блокировки* – определяет число неудачных попыток доступа к ОО, после которых учетная запись пользователя блокируется. Прежде чем увеличить счетчик блокировки, ОО сверяет неправильный пароль с теми, которые хранятся в истории паролей. Если неправильный пароль совпадет с любой из двух последних записей, которые хранятся в истории

паролей, то увеличение счетчика блокировки не осуществляется. Это возможность позволяет уменьшить количество блокировок, возникающих в результате пользовательских ошибок при вводе пароля. Блокированную учетную запись нельзя использовать до тех пор, пока администратором не будет сброшена блокировка или пока не истечет интервал блокировки. Значение для данного параметра может быть определено в диапазоне от 1 до 999. Установив число символов равным 0 можно запретить блокировку данной учетной записи. Попытки доступа к заблокированным сеансам, защищенным паролем, с неверным паролем не считаются неудачными попытками доступа к ОО. По умолчанию значение данного параметра установлено равным 0;

– *временной интервал, после которого произойдет сброс счетчика блокировки* – определяет число минут, которые должны пройти после неудачной попытки доступа к ОО, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше временного интервала блокировки учетной записи. По умолчанию данный параметр не определен.

**Политика Kerberos**

Политика Kerberos используется только в отношении учетных записей домена (политика Kerberos не входит в состав политики локального компьютера) и позволяет определять следующие параметры безопасности:

– *максимальная погрешность синхронизации часов компьютера* – определяет максимально допустимое протоколом аутентификации Kerberos расхождение (в минутах) между показаниями часов клиентского компьютера и функционирующего под управлением ОО контроллера домена, обеспечивающего проверку подлинности Kerberos. Данный параметр политики предотвращает реализацию сетевых атак, основанных на повторном воспроизведении трафика. Уполномоченный администратор посредством указанной политики может установить максимальный допуск рассогласования системного времени на компьютерах, приемлемый для протокола Kerberos.

Таким образом, если расхождение между показаниями часов клиентского компьютера и контроллера домена меньше значения, определяемого этой политикой значения, любая отметка времени, используемая в сеансе связи между двумя компьютерами, будет считаться достоверной. В противном случае, регистрация пользователя в домене будет невозможна. По умолчанию значение данного параметра политики установлено равным 5 минутам;

- *максимальный срок жизни билета пользователя* – определяет максимальный интервал времени (в часах) в течение которого действует пользовательский билет TGT (ticket-granting ticket – билет на выдачу билета). По истечении срока действия билета TGT необходимо запросить новый билет или возобновить существующий. По умолчанию значение данного параметра политики установлено равным 10 часам;
- *максимальный срок жизни билета службы* – определяет максимальный интервал времени (в минутах) в течение которого полученный билет сеанса разрешается использовать для доступа к конкретной службе. Это значение должно быть больше 10 минут, но не превышать значения «Максимальный срок жизни билета пользователя». По умолчанию значение данного параметра политики установлено равным 600 минутам;
- *максимальный срок жизни для возобновления билета пользователя* – определяет период времени (в днях) в течение которого можно возобновить пользовательский билет TGT. По умолчанию значение данного параметра политики установлено равным 7 дням;
- *принудительное ограничение доступа пользователя* – определяет, должен ли центр распределения ключей Kerberos проверять каждый запрос билета сеанса на соответствие политике прав, действующей в отношении учетных записей пользователей. По умолчанию данный параметр политики включен.

Данные политики позволяют ОО реализовывать единый механизм безопасности для всех пользователей, осуществлять централизованное управление без необходимости управления каждым из них в отдельности. Например, ОО автоматически потребует смену пароля для каждого пользователя по истечению максимального срока действия пароля. Таким же образом, при достижении порогового значения ошибок доступа к ОО учетная

запись пользователя будет заблокирована и в последующем разблокирована через установленный интервал времени.

#### 6.1.3.5 Стойкость аутентификации

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

**Сопоставление с ФТБ**

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

- FIA_AFL.1 – ФБО обнаруживают, когда происходит установленное администратором ОС число (не более 10) неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя, при достижении установленного числа неуспешных попыток аутентификации функции безопасности ОО осуществляют блокировку регистрационной записи пользователя ОО на 30 минут;
- FIA_ATD.1 – ФБО поддерживают базу данных атрибутов пользователей, в которой полностью определены учетные записи пользователей. Каждая учетная запись представлена в данной базе набором атрибутов: идентификатором безопасности, принадлежностью к группе, привилегиями, правами доступа к ОО, а также другой информацией;
- FIA_SOS.1 – ФБО предоставляют механизм для верификации качества паролей на доступ к ОО;
- FIA_UAU.2 – ФБО обеспечивают аутентификацию до любых действий субъектов доступа к ОО;

- FIA_UAU.7 – с целью предотвращения раскрытия пароля субъекта доступа во время интерактивной аутентификации ФБО обеспечивают отображение вводимого пароля в виде символов «*»;
- FIA_UID.2 – ФБО осуществляют идентификацию субъектов доступа к ОО до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого субъекта доступа;
- FIA_USB.1 (EXT) – 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;
- FTP_TRP.1 – ФБО обеспечивают защищенный от подмены механизм запроса на доступ к ОО (нажатие комбинации клавиш Ctrl-Alt-Del), который обеспечивает прямое взаимодействие пользователя с ФБО с целью передачи регистрационной информации и интерактивного доступа к ОО.

### 6.1.4 Функции безопасности «Управление безопасностью»

Объект оценки поддерживает ролевую модель, делегирование прав управления безопасностью, групповую политику, 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 состав участников группы. При осуществлении доступа к ОО пользователю присваивается определенная роль, для которой определено членство в группах и установлены привилегии. Несмотря на то, что в ОО могут быть определены различные роли, в ЗБ рассматриваются две логические роли: 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,

доменную группу безопасности «Администраторы домена». Пользователю будут предоставлены полномочия администратора только в том случае, если он зарегистрируется под той учетной записью, для которой определены соответствующие привилегии или которая является членом соответствующей административной группы.

Объект оценки поддерживает ряд локальных (в случае функционирования ОО на рядовом сервере, не являющемся контроллером домена) и доменных групп безопасности. Локальные группы используются для предоставления их членам прав на выполнение действий на локальном компьютере. Доменные группы безопасности являются частью Active Directory и характеризуются областью действия, которая описывает пределы применения группы в дереве доменов или в лесу. В таблице 6.7 перечислены локальные группы безопасности, создаваемые в момент установки ОО, и представлено описание их возможностей.

Таблица 6.7 – Локальные группы безопасности.

| Локальная группа | Описание |
|---|---|
| Администраторы (Administrators) | Члены данной группы имеют неограниченные права управления локальным компьютером интерактивно либо удаленно. По умолчанию членами данной группы является встроенная учетная запись администратора и любой член доменной группы «Администраторы домена» (Domain Admins). |
| Операторы архива (Backup Operators) | Члены этой группы могут выполнять доступ к ОО локально или удаленно, выполнять резервное копирование и восстановление системных данных, файлов и папок, а также завершать работу ОО. Операторы архива могут перекрывать ограничения доступа только в целях резервного копирования и восстановления файлов. |
| Гости (Guest) | Члены этой группы могут:<br>– выполнять только те задачи, для которых им предоставлены права;<br>– пользоваться только теми активами, на доступ к которым они имеют разрешения.<br>Члены этой группы не могут производить изменения рабочего стола. По умолчанию встроенная гостевая учетная запись «Гость» является членом этой группы. Учетная запись «Гость» по умолчанию отключена в ОО. |

| Локальная группа | Описание |
|---|---|
| Операторы настройки сети (Network Configuration Operators) | Члены этой группы могут вносить изменения в сетевые настройки ОО, а также обновлять и освобождать IP-адреса, если компьютер является сервером DHCP. По умолчанию эта группа не имеет членов. |
| Пользователи системного монитора (Performance Monitor Users) | Члены данной группы могут отслеживать (просматривать) счетчики производительности на локальном компьютере. По умолчанию эта группа не имеет членов. |
| Пользователи журналов производительности (Performance Log Users) | Члены этой группы могут управлять счетчиками, журналами и оповещениями производительности. Единственным членом данной группы является NT Authority\Network Service. |
| Опытные пользователи (Power Users) | Члены этой группы могут создавать и изменять локальные учетные записи пользователей в ОО и управлять совместно используемыми ресурсами. |
| Пользователи удаленного рабочего стола (Remote Desktop Users) | Членам данной группы разрешается выполнять вход на компьютер удаленным образом с использованием удаленного рабочего стола. |
| Репликатор (Replicator) | Обеспечивает функции репликации файлов в домене. |
| Пользователи (Users) | Члены этой группы могут выполнять только базовые задачи, такие как запуск приложений, использование принтеров, и пользоваться только теми ресурсами, на доступ к которым они имеют разрешения. По умолчанию ОО добавляет в группу «Пользователи» все локальные учетные записи пользователей, которые создаются в ОО. |
| Клиенты Telnet (Telnet Clients) | Члены данной группы могут использовать службу Telnet Server (Сервер Telnet) на локальном компьютере |

Доменные группы безопасности по типу и области действия делятся на следующие группы:

– доменные локальные (domain local);
– глобальные (global);

– универсальные (universal).

Доменные локальные группы безопасности главным образом используются для назначения глобальным группам разрешений на доступ к локальным активам домена. Доменные локальные группы безопасности доступны в пределах всего домена и могут содержать участников безопасности из любого домена в пределах леса, из доверенных доменов в других лесах и доменов более низкого уровня.

Глобальные группы в основном используются для предоставления членства в доменных локальных группах безопасности для отдельных участников безопасности и для прямого назначения разрешений на доступ к ресурсам домена. Глобальные группы применяются для объединения пользователей или компьютеров в одном домене и совместного исполнения одной роли или функции. Глобальные группы безопасности могут содержать только членов из своего домена.

Универсальные группы применяют для предоставления доступа к активам во всех доверенных доменах и могут содержать участников безопасности из любого домена в лесу.

Помимо локальных и доменных групп в ОО создаются специальные группы (special identity), которые управляются самим ОО. Специальные группы не имеют определенных членств, которые можно изменять, но в них входят различные пользователи в разные моменты времени в зависимости от того, каким образом пользователь получил доступ к ОО или активам. В таблице 6.9 перечислены специальные группы, поддерживаемые ОО.

Таблица 6.8 – Специальные группы.

| Специальная группа | Описание |
|---|---|
| Все (Everyone) | Представляет всех пользователей сети, в том числе осуществивших доступ под гостевой учетной записью, а также пользователей из других доменов. Каждый раз при доступе к ОО пользователь автоматически добавляется в группу «Все». |
| Прошедшие проверку (Authenticated Users) | В эту группу входят все пользователи, обладающие действительными учетными записями. |
| Создатель-владелец (Creator-Owner) | В данную группу включена учетная запись пользователя, создавшего объект или получившего право владения им. Если объект создан администратором, то им владеет группа |

| Специальная группа | Описание |
|---|---|
| | «Администраторы». |
| Сеть (Network) | Представляет пользователей, которые в настоящий момент обращаются к активам удаленно по сети (в отличие от тех, кто обращается к активам локально). При любом обращении к активам по сети пользователь автоматически добавляется в специальную группу «Сеть». |
| Интерактивные (Interactive) | Представляет всех пользователей, которые осуществили доступ к ОО. Члены интерактивной группы могут пользоваться активами ОО. При входе в ОО они получают доступ к активам компьютера «интерактивно». |
| Анонимный вход (Anonymous Logon) | Любая учетная запись, подлинность которой не может быть подтверждена ОО. |
| Удаленный доступ (Dialup) | Представляет любого пользователя, имеющего в настоящее подключение к сети через коммутируемое соединение. |

Любой пользователь, осуществивший доступ к ОО и не выступающий в роли администратора, рассматривается в роли пользователя.

#### 6.1.4.2 Делегирование управления

Делегирование прав управления безопасностью позволяет предоставлять пользователям ОО, не являющимся администраторами ОО, делегировать (передавать) определенные административные функции. Данный подход обеспечивает распределение административных задач среди соответствующих групп пользователей, не представляя никому их них полных административных полномочий.

Объект оценки позволяет передавать управление объектами Active Directory, представляя пользователю разрешения на:

- изменение свойств определенного контейнера Active Directory;
- создание, изменение или удаление объектов определенного класса в конкретном организационном подразделении – объекте-контейнере, используемом для объединения объектов домена в логические группы;
- изменение определенных свойств объектов заданного класса в определенном ОП или контейнере.

### 6.1.4.3 Групповая политика

Цель политик безопасности – определить процедуры выбора конфигурации и управления безопасностью в среде функционирования. Групповая политика помогает применить технические рекомендации в политике безопасности для всех клиентских компьютеров и серверов в доменах Active Directory.

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 клиентских 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. Использование групповой политики в сочетании со структурой организационных подразделений позволяет определять специфические настройки безопасности для тех или иных функций конкретного клиентского компьютера или сервера.

В случае использования групповой политики для создания настроек безопасности любые изменения, осуществляемые по отношению к какой-либо из политик, будут относиться ко всем серверам и клиентским компьютерам, использующим эту политику.

Групповая политика может быть применена не однократно в пределах домена, а многократно к разным элементам в иерархии Active Directory. Достигается это за счет объектов групповой политики (ОГП) – наборов параметров групповой политики. Параметры групповой политики хранятся на контроллере домена в папках совместно используемого объекта SYSVOL и контейнерах в Active Directory. Соответственно и сами групповые политики состоят из двух частей: контейнеров групповой политики Group Policy Container (GPC) и шаблонов групповой политики Group Policy Template (GPT). Для каждого ОГП в каталоге Active Directory имеется свой контейнер.

На каждом компьютере, функционирующем под управлением ОО, имеется один локальный (local) ОГП. Кроме того, на компьютер может распространяться действия множества нелокальных (nonlocal) ОГП, основанных на службе каталогов Active Directory.

Локальный ОГП храниться на компьютере независимо от того, работает последний в сети и есть ли сведения о нем в службе каталогов Active Directory. Тем не менее, поскольку нелокальные ОГП могут перекрывать параметры локального ОГП, в среде Active Directory данные параметры меньше всего влияют на параметры безопасности и конфигурацию ОО. В изолированной среде (или в вычислительной сети, не имеющей контроллера домена) параметры локального ОГП приоритетнее и нелокальные ОГП не могут их перекрыть.

Нелокальные ОГП связаны с объектами Active Directory (сайтами, доменами или ОП). В Active Directory параметры политик из нелокальных ОГП суммируются и применяются в соответствие с иерархией объектов Active Directory: от сайтов к ОП.

Существуют два вида параметров групповой политики: конфигурационные параметры компьютера (computer configuration setting), служащие для настройки политик, действия которых распространяются на компьютеры независимо от того, какой пользователь зарегистрирован в ОО, и пользовательские конфигурационные параметры, служащие для настройки политик, распространяющихся на пользователей, независимо от компьютера, на котором они регистрируются. Для настройки конфигурационных параметров компьютера и пользовательских параметров используются следующие узлы пространства имен ОГП:

- Конфигурация программ (Software settings);
- Конфигурация Windows (Windows settings);
- Административные шаблоны (Administrative Templates).

Узел «Конфигурация программ» позволяет определить порядок установки и поддержки программного обеспечения. Управлять приложениями можно в одном из двух режимов – назначения или публикации. Приложение назначается, когда необходимо, чтобы оно было установлено на всех компьютерах. Приложение публикуется, когда необходимо сделать его доступным для тех пользователей, управляемых данным объектом групповой политики, кому необходимо установить это приложение. При публикации приложения каждый пользователь определяет необходимость установки приложения самостоятельно.

Через узел «Конфигурация Windows» определяются сценарии, исполняемые при запуске и завершении работы компьютера, а также при входе/выходе пользователя в/из

системы. В первом случае выполнение сценариев осуществляется с правами локальной системы, во втором – с правами пользователя, выполняющего вход/выход в/из системы.

Кроме того, в данном узле пространства имен ОГП в разделе «Параметры безопасности» для ОП, домена или сайта могут быть определены различные политики безопасности, включая проверку подлинности пользователя при регистрации в ОО, принадлежность пользователя определенным группам, права доступа к защищаемым активам, политику аудита событий безопасности и т.д.

Узел «Административные шаблоны» содержит конфигурационные параметры, позволяющие уполномоченному администратору ОО управлять функциями доступа к ОО и завершением сеанса, самой групповой политикой, параметрами сетевых подключений, администрировать компоненты ОО (включая, NetMeeting, Internet Explorer, Windows Installer) и др.

#### 6.1.4.4 Функции управления безопасностью

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

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

**Политика учетных записей** – функции управления политикой учетных записей предоставляют уполномоченным администраторам ОО возможность устанавливать ограничения на применяемые пароли, определять параметры блокировки учетных записей

и политику Kerberos. Определяя политику использования паролей, уполномоченный администратор ОО задает минимальную длину пароля, требование неповторяемости паролей, минимальный и максимальный срок действия пароля. В случае превышения максимального срока действия пароля пользователь не сможет осуществить доступ к ОО до того момента, пока не сменит пароль. Параметры блокировки учетных записей определяют пороговое значение неуспешных попыток доступа к ОО, при превышении которого учетная запись будет заблокирована, продолжительность блокировки и интервал времени, после которого произойдет сброс счетчика блокировки. Параметры политики Kerberos определяют характеристики протокола аутентификации Kerberos.

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

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

**Политика управления доменом** – функции управления доменом (домен – основная административная единица службы каталогов Active Directory) позволяют уполномоченному администратору ОО добавлять и удалять компьютеры из состава домена, а также управлять доверительными отношениями (trust) с другими доменами леса или лесами доменов.

**Политика управления дисковыми квотами** – функции управления дисковыми квотами позволяют уполномоченному администратору управлять дисковыми квотами на

томах файловой системы. Уполномоченный администратор ОО имеет возможность включать или отключать использование дисковых квот, определять размер дисковых квот, устанавливаемых по умолчанию, а также задавать требуемое действие при превышении пользователя выделенного объема квот.

**Групповая политика –** функции управления групповой политикой позволяют уполномоченному администратору ОО централизованно управлять параметрами безопасности ОО, конфигурационными изменениями ОО, развертывать программное обеспечение и определять его поведение.

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

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

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

**Сопоставление с ФТБ**

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

- FMT_MOF.1 – ФБО предоставляют возможность выполнять определенные действия над функциями из числа ФБО в части управляемых характеристик безопасности только уполномоченным администраторам безопасности, перечень действий, функций и управляемых характеристик приведен в таблице 5.3;
- FMT_MSA.1 (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.1 (2) – ФБО предоставляют возможность модифицировать атрибуты управления доступом, ассоциированные с именованным объектом, используемые при реализации политики дискреционного управления доступом, только пользователю ОО, являющемуся владельцем объекта; пользователю ОО, имеющему право смены владельца; пользователю ОО, имеющему право модификации DACL;
- FMT_MSA.1 (3) – ФБО предоставляют возможность модифицировать и удалять атрибуты безопасности, используемые при реализации политики фильтрации информации, только уполномоченному администратору ОО;
- FMT_MSA.1 (4) – ФБО предоставляют возможность удалять, создавать атрибуты безопасности для правил управления информационными потоками, используемых в политике фильтрации информации;
- 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.3 (2) – ФБО устанавливают запрет на все входящие информационные потоки по умолчанию при инициализации брандмауэра

сетевых подключений, только уполномоченному администратору ОО доступны возможности по дальнейшей модификации политики фильтрации;

- FMT_MTD.1 (1) – ФБО предоставляют возможность выполнять операции над данными ФБО согласно таблице 5.4 только уполномоченному администратору ОО;
- FMT_MTD.1 (2) – ФБО предоставляют возможность уполномоченному пользователю ОО выполнять модификацию собственных аутентификационных данных;
- FMT_MTD.2 – ФБО предоставляют уполномоченному администратору ОО возможность определять пороговое значение количества неуспешных попыток аутентификации, при превышении установленного порогового значения ФБО должны блокировать учетную запись пользователя на время, определенное администратором ОО;
- FMT_REV.1 (1) – ФБО предоставляют возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО, администраторами ОО и объектами, только уполномоченному администратору ОО и осуществляют правила отмены полномочий у пользователей ОО и администраторов ОО на доступ к объектам, а также правила отмены прав доступа к объекту (модификацию списка дискреционного доступа);
- FMT_REV.1 (2) – ФБО предоставляют возможность отмены атрибутов безопасности, ассоциированных с объектами, только пользователю ОО, уполномоченному согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта, и осуществляют правила отмены прав доступа к объекту (модификацию списка дискреционного доступа);
- FMT_SAE.1 – ФБО предоставляют возможность назначать срок действия аутентификационных данных только уполномоченному администратору ОО, ФБО осуществляют блокирование ассоциированной с пользователем учетной записи по истечении срока действия аутентификационных данных;
- FMT_SMR.1 – ФБО поддерживают ролевую модель, определяя роль администратора ОО и пользователя ОО.

### 6.1.5 Функции безопасности «Защита ФБО»

Функции безопасности ОО «Защита ФБО» обеспечивают:

– отказоустойчивость ОО;
– репликацию изменений безопасности;
– целостность системы;
– доступ к объекту посредством описателей;
– разделение доменов;
– службу времени.

#### 6.1.5.1 Отказоустойчивость ОО

Отказоустойчивость ОО обеспечивается с помощью технологий кластеризации.

ОО включает в себя возможность использования двух средств кластеризации:

– Отказоустойчивые кластеры;
– Балансировка сетевой нагрузки.

В случае возникновения сбоев (при условии установки одного из типов кластеризации на ОО) на одном из узлов кластера все данные ОО, в том числе и ФБО с установленными параметрами, передаются на работающий активный узел кластера, тем самым обеспечивается непрерывность функционирования ОО.

#### 6.1.5.2 Репликация изменений безопасности

Все изменения, связанные с безопасным состоянием ОО (блокирование учетной записи, изменение пароля доступа и др.) тиражируются (реплицируются) на все серверы, выполняющие роль контроллеров домена. Таким образом, все контроллеры домена оповещаются о текущем состоянии безопасности.

Указанная функциональная возможность ОО обеспечивается поддержкой различных видов репликации, рассматриваемых в настоящем пункте ЗБ.

**Немедленная репликация**

При смене пароля пользователя информация об этом немедленно посылается по безопасному каналу Netlogon на контроллер домена – хозяин эмулятора PDC (Primary

Domain Controller). Хозяин эмулятора PDC (PDC emulator operations master) получает предпочтительную репликацию изменений паролей, произведенных другими контроллерами домена, и управляет всеми запросами проверки подлинности, не прошедшими на контроллерах домена. В любой момент времени в отдельном домене может быть только один хозяин эмулятора PDC.

Фактически контроллер домена посылает хозяину эмулятора PDC удаленный вызов процедуры (RPC), включающий имя пользователя и информацию о новом пароле. Хозяин эмулятора PDC сохраняет это значение локально в собственной реплике каталога Active Directory.

Немедленная репликация данных между контроллерами домена, функционирующими под управлением ОО, связана со следующими событиями:

- блокировка учетной записи;
- изменение в секретном ключе локального администратора безопасности (Local Security Authority);
- изменение в состоянии диспетчера относительных идентификаторов RID (Relative ID Manager).

**Срочная репликация**

Репликация Active Directory происходит между контроллерами домена, когда данные каталога обновляются на одном контроллере домена и это обновление тиражируется на все другие контроллеры домена. Когда происходит изменение данных каталога, исходный контроллер домена посылает уведомление о том, что его хранилище каталога теперь содержит обновленные данные. После этого партнеры контроллера домена по репликации посылают ему запрос на передачу изменений. Обычно контроллер исходного домена посылает уведомление об изменениях с некоторой задержкой. Эта задержка определяется заданной задержкой уведомления (по умолчанию задержка уведомления в ОО составляет 15 секунд с трехсекундным смещением интервала репликации для разных сайтов). Однако для некоторых видов изменений любая задержка в репликации может привести к снижению уровня безопасности. Срочная репликация обеспечивает немедленное тиражирование самых важных изменений в каталоге, включая блокировку учетных записей, изменения в политике блокировки учетных записей,

изменения в политике паролей домена и изменения, связанные с паролем учетной записи контроллера домена. При срочной репликации уведомление об обновлении отсылается немедленно, независимо от значения задержки уведомления. Такой подход позволяет другим контроллерам домена немедленно запрашивать и получать информацию о самых важных изменениях.

Единственное различие между срочной репликацией и обычной репликацией заключается в отсутствии задержки перед передачей уведомления об изменениях.

Когда уполномоченный администратор ОО производит разблокирование учетной записи, вручную прекращает срок действия пароля учетной записи пользователя или меняет пароль учетной записи, измененные параметры немедленно передаются хозяину эмулятора PDC, после чего происходит их срочная репликация на другие контроллеры домена, находящиеся в том же сайте, что и эмулятор PDC. По умолчанию срочная репликация не переходит за границы сайтов.

Следующие события подлежат срочной репликации:

– изменение политики блокировки учетной записи;
– изменение политики паролей домена;
– изменение пароля учетной записи компьютера.

**Репликация одного объекта-пользователя «по требованию»**

В ОО, когда уполномоченный администратор ОО сбрасывает прежний пароль и немедленно прекращает действие нового пароля пользователя на контроллере домена в одном сайте (т.е. новый пароль пользователю предоставляется, но он должен поменять его при первом входе в ОО), пользователь может успешно войти в систему с новым паролем в другом сайте. Это происходит вследствие того, что в ходе проверки подлинности контроллер домена передает информацию на контроллер – хозяин эмулятора PDC.

Однако изменения в пароле пользователя могут неправильно реплицироваться. Это происходит из-за того, что репликация между сайтами происходит с некоторой задержкой.

Поддерживаемая ОО схема репликации позволяет контроллеру домена связаться с хозяином эмулятора PDC и запросить обновление объекта-пользователя, не прошедшего проверку подлинности из-за неправильного пароля. Таким образом, контроллер домена,

проверяющий подлинность пользователя, сразу получает самую свежую информацию об учетной записи пользователя.

Схема и описание последовательности действий по проверки подлинности аутентификационной информации контроллером – хозяином эмулятора PDC представлено ниже (см. рисунок 6.6).

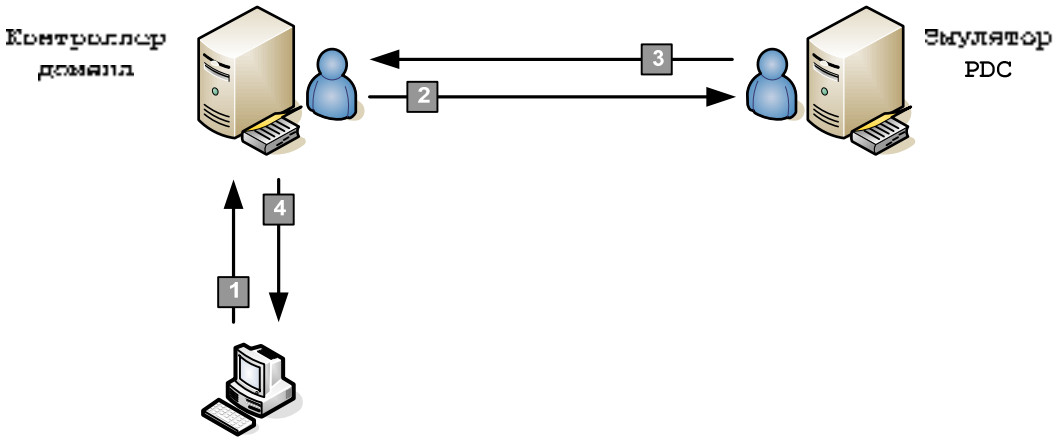



Рисунок 6.6 – Схема проверки подлинности аутентификационной информации хозяином эмулятора PDC.

1. Клиентский компьютер передает учетные данные пользователя на контроллер домена. Эта информация состоит из имени пользователя и пароля.

2. Если контроллер домена обнаруживает, что проверка подлинности не пройдена и возвращено соответствующее условие (STATUS_WRONG_PASSWORD, STATUS_ PASSWORD_EXPIRED, STATUS_PASSWORD_MUST_CHANGE или STATUS_ACCOUNT_ LOCKED_OUT), он пытается провести проверку подлинности с помощью хозяина эмулятора PDC. Иными словами, контроллер домена запрашивает PDC определение, является ли проверяемый пароль действительным. Контроллеру домена требуется эта информация от PDC, так как сам он может не иметь текущего пароля пользователя, а хозяин эмулятора PDC всегда располагает актуальным значением пароля.

3. Проверка подлинности проводится заново хозяином операций эмулятора PDC, и на этом этапе определяется правильность пароля. Окончательное решение о достоверности пользовательского пароля принимает контроллер PDC. Информация о результатах проверки подлинности передается хозяином эмулятора PDC на проверяющий контроллер домена.

4. Затем проверяющий контроллер домена посылает на клиентский компьютер уведомление об успешной или неуспешной попытке входа в систему.

#### 6.1.5.3 Целостность системы

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

#### 6.1.5.4 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 политике 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.

#### 6.1.5.5 Разделение доменов

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

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

Управление аппаратными средствами ФБО осуществляется программным обеспечением ФБО режима ядра. Аппаратные средства ФБО не могут быть модифицированы недоверенными субъектами. Защита программного обеспечения ФБО режима ядра от модификации обеспечивается посредством контроля состояния функционирования аппаратных средств и защитой памяти. Аппаратные средства ФБО обеспечивают инструкции, генерирующие программные прерывания, позволяющие переходить из состояния режима пользователя в состояние режима ядра. Программное обеспечение ФБО режима ядра осуществляет обработку всех прерываний и определяет обоснованность сделанных вызовов в режиме ядра. Механизм защиты памяти реализован таким образом, что напрямую обращаться к памяти могут только компоненты в режиме ядра. Прямое взаимодействие с памятью внешних подсистем и приложений пользовательского режима невозможно.

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

ФБО обеспечивают изоляцию всех виртуальных машин друг от друга и от вмешательства в процесс функционирования виртуальных машин недоверенных пользователей или пользователей, не работающих в области действия виртуальной машины.

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

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

#### 6.1.5.6 Служба времени

Поддерживаемая ОО аппаратная платформа включает контроллер часов реального времени, представляющий устройство, доступ к которому может быть возможен 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 (например, контроллером домена). Возможность запроса времени ничем не ограничена, в то время как изменение системного времени требует полномочий на выполнение данной операции. Данная привилегия предоставлена только уполномоченным администраторам ОО с целью обеспечения непротиворечивости службы времени.

Служба времени Windows (W32Time) обеспечивает управление синхронизацией даты и времени на всех клиентах и серверах при функционировании ОО в домене Active Directory. Если данная служба остановлена, синхронизация даты и времени будет недоступна. Если эта служба отключена, любые службы, которые явно зависят от нее, не могут быть запущены. Служба времени Windows гарантирует корректность установленного в ОО времени и его синхронизацию с контроллерами домена в домене. Это необходимое условие при аутентификации по протоколу аутентификации Kerberos, а также для обеспечения согласованности регистрируемых в журнал аудита событий безопасности.

Служба времени Windows обеспечивает управление синхронизацией даты и времени посредством протокола SNTP (Simple Network Time Protocole). При функционировании ОО в доменной среде механизм синхронизации времени осуществляется следующим образом:

- хозяин эмулятора PDC (Primary Domain Controller) корневого домена леса выступает как источник информации о точном времени для всей сети в целом;
- эмуляторы PDC других доменов леса, расположенных ниже по иерархии относительно корневого домена, в качестве источника синхронизации времени выбирают эмулятор PDC корневого домена;
- в свою очередь все контроллеры домена синхронизируют свое время с контроллером домена, выполняющим роль эмулятора PDC в собственном домене;
- все остальные компьютеры используют контроллер собственного домена в качестве источника точного времени.

Эмулятор PDC корневого домена леса может быть синхронизирован с внешним сервером времени либо с собственным контроллером часов реального времени.

**Сопоставление с ФТБ**

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

- FPT_ATM.1 – ФБО осуществляют тестирование функционирования (аппаратной части), критичной по безопасности, в процессе загрузки ОО и по требованию уполномоченного администратора ОО;
- FPT_FLS.1 – ФБО должны сохранять безопасное состояние в случае возникновения сбоев;
- FPT_ITT.1 – ФБО обеспечивают защищенную репликацию данных ФБО между ОО и всеми компьютерами с установленными релизами ОО (в случае совместного обеспечения безопасности, осуществляемого ОО и указанными компьютерами);
- FPT_RCV.1 – ФБО предоставляют возможность и средства для уполномоченного администратора, позволяющие осуществить возврат ОО в безопасное состояние в случае сбоя или прерывания обслуживания;
- FPT_RVM.1 – ФБО обеспечивают, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ;

- FPT_SEP.1 – ФБО обеспечивают поддержание домена безопасности для собственного выполнения, защищающего их от вмешательства и искажения недоверенными субъектами;
- FPT_SSP.1 – в случае функционирования ОО совместно с другими экземплярами ОО, установленными на компьютерах (контроллерах домена) для решения задач совместного с ОО обеспечения безопасности информации (например, в составе одного домена), ОО обеспечивает возможность проведения надлежащей согласованной синхронизации состояния безопасности (репликации), вызванной изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО;
- FPT_STM.1 – контроллер часов реального времени, реализованный на аппаратной платформе ОО, в сочетании с периодической синхронизацией с внешним источником времени и возможностью их изменения только администратором ОО, предоставляют надежные метки времени для ФБО;
- FPT_TDC.1 – ФБО предоставляют возможность управления клиентскими и серверными ОС и обеспечивают согласованную интерпретацию совместно используемых данных ФБО: идентификационной и аутентификационной информации, информации авторизации, настроек безопасности, а также управляющих и служебных данных, необходимых для безопасного функционирования ОО, клиентских и серверных ОС;
- FPT_TRC.1 – в случае совместного обеспечения безопасности ОО и других компьютеров (например, функционирование в составе одного домена и в ролях контроллеров домена) ФБО обеспечивают согласованность данных ФБО в случае восстановления прерванного соединения с компьютерами, функционирующими под управлением других экземпляров ОО;
- FPT_TST.1 – ФБО осуществляют самотестирование в процессе запуска ОО и по требованию уполномоченного пользователя в процессе функционирования;
- VDS_VMM.1. (EXT) ФБО должно поддерживать домен безопасности для функционирования каждой виртуальной машины, который должен защищать виртуальную машину от вмешательства и искажения недоверенными субъектами или субъектами, находящимися вне области действия виртуальной

машины. ФБО должно реализовывать разделение между доменами безопасности виртуальных машин в ОДФ.

### 6.1.6 Функции безопасности ОО «Использование ресурсов ОО»

Объект оценки предоставляет возможность ограничивать на определенном томе NTFS объем доступного для пользователя дискового пространства. Любой том NTFS обладает набором свойств, включая информацию об используемых дисковых квотах, которые могут быть изменены только уполномоченным администратором. Данные свойства позволяют уполномоченному администратору разрешать или запрещать использование дисковых квот на выбранном томе, указывать размер квоты, выделяемой по умолчанию, задавать порог выдачи предупреждений и определять действие при превышении квоты.

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

Уполномоченные администраторы могут настроить ОО таким образом, чтобы:

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

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

Используемое дисковое пространство ассоциируется с учетной записью пользователя ОО, «владеющего» им, на основе атрибута объекта, определяющего его владельца. При первом создании пользователем объекта на томе с разрешенным квотированием для его учетной записи создается запись квоты (если она не была создана

явным образом). Эта запись квоты изначально задает дисковое пространство, выделяемое по умолчанию, определяет порог выдачи предупреждений и в дальнейшем используется для управления дисковым пространством, установленным для учетной записи пользователя. Каждый раз, когда для данной учетной записи необходимо выделить дисковое пространство (например, при создании или изменении объекта), проверяется размер выделенной квоты, порог предупреждений и происходит изменение записи квоты для этой учетной записи. При превышении порога выдачи предупреждений или установленного размера выделенных квот, выполняются определенные администратором ОО действия.

Объект оценки обеспечивает поддержку режима квотирование для объектов Active Directory, управляя, таким образом, количеством объектов, которые могут принадлежать указанному разделу каталога Active Directory. На членов групп безопасности «Администраторы домена» и «Администраторы предприятия» ограничения, определяемые политикой квотирования, не распространяются.

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

Объект оценки обеспечивает отказоустойчивость на уровне системы, которая представлена двумя технологиями кластеризации:

– Отказоустойчивые кластеры;
– Балансировка сетевой нагрузки.

**Отказоустойчивые кластеры.**

Отказоустойчивые кластеры, позволяют обеспечивать отказоустойчивость на уровне системы с помощью процесса, называемого подхватом функций. Отказоустойчивые кластеры используются для доступа к ресурсам: общие файловые ресурсы, очереди печати, служб электронной почты, служб баз данных и серверных приложений. В случае появления проблем с каким-нибудь кластерным ресурсом служба отказоустойчивого кластера сначала пытается устранить ее путем перезапуска этого ресурса и всех остальных зависимых от него ресурсов. Если это не помогает, группа Services and Applications (Службы и приложения), членом которой является данный ресурс, переносится с помощью процесса подхвата функций на другой доступный узел в кластере, где он затем может быть запущен снова. Кластерные узлы могут следить за

состоянием ресурсов, функционирующих на их локальной системе, а также отслеживать и состояние других узлов в кластере посредством специальных пересылаемых по частной сети сообщений, которые называются сигналами активности (heartbeats). Обмен сигналами активности позволяет, как определять состояние узлов, так и отправлять информацию об этом и появившихся в конфигурации кластера изменениях механизму кворума кластера. В кворуме кластера содержатся конфигурационные данные, необходимые для восстановления кластера до рабочего состояния. Каждый узел в кластере должен иметь доступ к кворумному ресурсу. ОО поддерживает четыре разных модели кворума:

- Большинство узлов (Node Majority);
- Большинство узлов и дисков (Node and Disk Majority);
- Большинство узлов и общих файловых ресурсов (Node and Share Majority);
- Нет большинства: только диск (No Majority: Disk Only).

**Модель кворума Большинство узлов.**

Модель кворума Большинство узлов предназначена для развертывания отказоустойчивых кластеров с нечетным количеством кластерных узлов. При определении кворумного состояния кластера подсчитывается только количество доступных узлов. Такой кластер остается в рабочем и функциональном состоянии до тех пор, пока количество доступных узлов превышает количество отказавших узлов.

**Модель кворума Большинство узлов и дисков.**

В модели кворума Большинство узлов и дисков то, может ли кластер продолжать функционировать, определяется путем подсчета количества доступных узлов и проверки доступности кластерного диска-свидетеля. В случае применения этой модели, данные кластерного кворума сохраняются на кластерном диске, который имеется в наличии и делается доступным для всех узлов в кластере посредством общего устройства хранения (shared storage device) с помощью соединений SAS (Serial Attached SCSI – SCSI с последовательным интерфейсом) Fibre Channel или ISCI.

**Модель кворума Большинство узлов и общих файловых ресурсов.**

Модель кворума Большинство узлов и общих файловых ресурсов очень похожа на модель Большинство узлов и дисков, но только подразумевает сохранение данных кворума не на диске-свидетеле, а в общем файловом ресурсе.

**Модель кворума Нет большинства: только диск.**

Модель кворума Нет большинства: только диск предназначена для тестирования процесса и поведения, связанного с развертыванием в отказоустойчивом кластере каких-нибудь встроенных или специальных служб и/или приложений. Такая модель кластера может выдержать отказы всех узлов кроме одного, при условии, если диск, на котором содержатся данные кворума, остается доступным.

**Балансировка сетевой нагрузки.**

Балансировка сетевой нагрузки (NLB) обеспечивает высокую производительность и доступность сети за счет распределения клиентских запросов между несколькими серверами. При увеличении клиентской нагрузки кластеры NLB могут расширяться путем добавления в кластер дополнительных узлов для поддержания или улучшения времени отклика на клиентские запросы.

**Сопоставление с ФТБ**

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

- FRU_FLT.2 – ФБО должно обеспечивать выполнение всех возможностей ОО, в случае возникновения сбоев;
- FRU_PRS.1 – ФБО дают возможность установить приоритет каждому процессу и обеспечивают доступ к процессорному ресурсу на основе приоритетов;
- FRU_RSA.1 – механизм квотирования на томах файловой системы и объектов службы каталогов предоставляет администратору ОО возможность эффективно ограничивать общий объем дискового пространства, которое доступно для пользователя ОО или группы пользователей, а также количество объектов, которые могут принадлежать указанному разделу каталога Active Directory.

### 6.1.7 Функции безопасности ОО «Блокирование сеанса»

Объект оценки предоставляет пользователям ОО возможность блокировать собственный интерактивный сеанс немедленно или по истечении определенного ими

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

С другой стороны, пользователи ОО могут блокировать собственный сеанс после настройки через свойства экрана режима заставки. Настройка свойства экрана режима заставки может осуществляться как вручную, так и с использованием параметра групповой политики «Таймаут экранной заставки», определяющего временной интервал бездействия пользователя ОО перед тем, как будет запущена экранная заставка, и параметра «Использовать парольную защиту для экранных заставок», определяющего необходимость использования парольной защиты экранных заставок на компьютерах.

Если эта политика включена, все экранные заставки будут использовать парольную защиту. Пользователь ОО может использовать в качестве заставки какую-либо программу, определять время неактивности, по истечении которого включится режим заставки, и задавать пароль, необходимый для возврата в сеанс пользователя ОО. ФБО непрерывно контролируют активность мыши и клавиатуры и, если они бездействуют в течение установленного пользователем ОО времени, ФБО инициируют режим заставки и блокируют сеанс пользователя ОО.

При блокировании сеанса вручную либо после каких-либо манипуляций мышью или нажатия клавиатуры в режиме заставки (предполагается, что для выхода из режима заставки требуется пароль, в противном случае произойдет немедленный возврат в сеанс), ФБО отобразят диалоговое окно входа, сообщающее о том, что пользователю ОО необходимо нажать комбинацию клавиш Ctrl-Alt-Del для повторного доступа к ОО. Независимо от того, как был заблокирован сеанс, пользователь ОО должен нажать комбинацию клавиш Ctrl-Alt-Del для вызова диалогового окна аутентификации. Далее пользователь ОО должен заново ввести пароль, который был хэширован при первоначальной регистрации, и, в случае ввода корректного пароля, пользователь ОО возобновляет собственный сеанс.

Объект оценки предоставляет уполномоченному администратору ОО возможность ввода собственного идентификатора и пароля для доступа к ОО. Если ФБО успешно

аутентифицируют администратора ОО, сеанс пользователя, уже выполнившего первоначальную регистрацию в ОО, будет завершен. Для администратора ОО будет создан новый сеанс.

**Сопоставление с ФТБ**

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

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

### 6.1.8 Функции безопасности ОО «Управление доступом к ОО»

Функции безопасности ОО «Управление доступом к ОО» обеспечивают возможность ограничения открытия сеанса доступа на основе идентификатора пользователя, времени доступа, имени компьютера, с которого осуществляется доступ к ОО и срока действия аутентификационных данных.

При открытии сеанса доступа пользователя ФБО осуществляют проверку разрешений на возможность осуществления данным субъектом доступа к ОО. Проверка осуществляется на основе идентификатора пользователя (login name), для которого администратором ОО определены разрешающие или запрещающие права доступа к ОО, времени доступа и имени компьютера, с которого осуществляется доступ к ОО.

Ограничение по времени доступа к ОО задается уполномоченным администратором ОО и заключается в определении временного интервала, в течение которого пользователю разрешен или запрещен доступ к ОО (к домену). Данный параметр

не влияет на возможность пользователя осуществлять доступ к ОО на локальном компьютере с использованием локальной ученой записи.

Ограничение по имени компьютера предоставляет уполномоченному администратору ОО инструмент управления режимом доступа к компьютеру с установленным ОО. Администратор имеет возможность разрешить пользователям доступ к ОО на всех рабочих станциях домена или всего леса доменов либо определить для учетной записи пользователя список компьютеров, доступ на которые разрешен.

При истечении срока действия аутентификационных данных, определяемого уполномоченным администратором ОО, ФБО запрещают доступ пользователей к ОО до проведения процедуры смены аутентификационных данных.

Объект оценки обеспечивает управление возможностью интерактивного локального доступа пользователя в систему с использованием параметров групповой политики «Локальный вход в систему» (определяет пользователей, имеющих возможность осуществлять интерактивный доступ к ОО) и «Отклонить локальный вход» (определяет, каким пользователям запрещается доступ к ОО). Параметр «Отклонить локальный вход» имеет больший приоритет, в случае если учетная запись пользователя контролируется обеими политиками.

**Сопоставление с ФТБ**

Функции безопасности «Управление доступом к ОО» удовлетворяют следующему функциональному требованию безопасности:

- FTA_TSE.1 – ФБО способны отказать в открытии сеанса доступа к ОО, основываясь на идентификаторе пользователя, имени компьютера, сроке действия аутентификационных данных и времени доступа к ОО.

## 6.2 Меры доверия к безопасности ОО

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

- управление конфигурацией;
- предоставление руководств;
- предоставление проектной документации;
- тестирование;

– оценка стойкости функций безопасности.

### 6.2.1 Управление конфигурацией

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

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

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

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

**Сопоставление с ТДБ**

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

– ACM_CAP.1.

### 6.2.2 Представление руководств

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.

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.

**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 отображение 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

ЗАО «АЛТЭКС-СОФТ» предоставляет ОО, пригодный для тестирования, с соответствующей документацией, это позволяет провести независимое тестирование ФБО и сделать заключение, выполняются ли ФБО в соответствии со спецификациями.

**Сопоставление с ТДБ**

Меры доверия, связанные с тестированием, удовлетворяют требованию доверия:

– ATE_IND.1.

### 6.2.5 Оценка стойкости функций безопасности

Для механизма парольной защиты, являющегося вероятностным, предоставляется материал анализа стойкости функции безопасности (аутентификации). Анализ стойкости функции безопасности представлен в документе «Операционная система Microsoft Windows Server 2008. Свидетельство анализа стойкости функций безопасности ОО. Версия 1.0, 2009, MS.Win_Srv2008.СФБ».

**Сопоставление с ТДБ**

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

– AVA_SOF.1.

# 7 Утверждения о соответствии ПЗ

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

## 7.1 Ссылка на ПЗ

Объект оценки соответствует профилю защиты ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

## 7.2 Конкретизация ПЗ

Все требования безопасности, сформулированные в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Эти операции завершены в настоящем ЗБ в полном объеме (см. таблицу 7.1 – компоненты требований с пометкой «завершено»).

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

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

Таблица 7.1 – Конкретизация функциональных требований по отношению к ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005».

| Наименование требования | Изменение |
|---|---|
| FAU_GEN.1 | завершено<br>уточнено |
| FAU_SAR.3 | завершено |
| FAU_SEL.1 | завершено |
| FAU_STG.3 | завершено |
| FAU_STG.4 | завершено |
| FDP_ACC.1 | завершено |
| FDP_ACF.1 | завершено<br>уточнено |
| FIA_AFL.1 | завершено |
| FIA_ATD.1 | завершено |
| FIA_SOS.1 | завершено |
| FIA_USB.1 (EXT) | завершено |
| FMT_MOF.1 | завершено |
| FMT_MSA.1 | завершено |
| FMT_MSA.3 | завершено |
| FMT_MTD.1 | завершено |
| FMT_MTD.2 | завершено |
| FMT_REV.1 (1) | завершено |
| FMT_REV.1 (2) | завершено |
| FMT_SAE.1 | завершено |
| FMT_SMR.1 | завершено |
| FPT_TDC.1 | завершено |
| FTA_TSE.1 | завершено |

## 7.3 Дополнение ПЗ

В настоящее ЗБ включены следующие угрозы, которым противостоит ОО, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

**T.FaultConformSrv**

**1. Аннотация угрозы –** нарушение режимов взаимодействия ОО и других экземпляров ОО, установленных на серверах для решения задач совместного с ОО обеспечения безопасности информации, вследствие несогласованной интерпретации совместно используемых данных ФБО.

**2. Источники угрозы –** программное обеспечение ОО.

**3. Способ реализации угрозы –** несогласованность в интерпретации совместно используемых данных ФБО.

**4. Используемые уязвимости –** недостатки механизмов ОО, обеспечивающих согласованную интерпретацию совместно используемых данных ФБО.

**5. Вид активов, потенциально подверженных угрозе –** данные ФБО; пользовательские данные; программное обеспечение ОО.

**6. Нарушаемое свойство безопасности активов –** целостность, доступность.

**7. Возможные последствия реализации угрозы –** нарушение режимов взаимодействия ОО и других экземпляров ОО, установленных на серверах для решения задач совместного с ОО обеспечения безопасности информации.

**T.UnauthUsageRes**

**1. Аннотация угрозы –** исчерпание свободных ресурсов ОО (вычислительные возможности, дисковое пространство) вследствие неограниченного их использования пользователями ОО.

**2. Источники угрозы –** пользователи ОО.

**3. Способ реализации угрозы –** генерация процессов, использующих вычислительны возможности ОО, и создание объектов, использующих дисковое пространство ОО, пользователями ОО.

**4. Используемые уязвимости –** недостатки механизмов надлежащего распределения ресурсов ОО, связанные с возможностью их исчерпания.

**5. Вид активов, потенциально подверженных угрозе –** ресурсы ОО.

**6. Нарушаемое свойство безопасности активов –** доступность.

**7. Возможные последствия реализации угрозы –** нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

В настоящее ЗБ включены следующие политики безопасности организации, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

**P.SynchrState**

В случае функционирования ОО и других экземпляров ОО, установленных на серверах, для совместного решения задач обеспечения безопасности информации и управления клиентскими и серверными ОС, должна быть обеспечена возможность проведения надлежащей синхронизации состояния безопасности, вызванной изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО.

**P.FiltrationFlow**

Должна осуществляться фильтрация входящих в ОО информационных потоков.

В настоящее ЗБ включены следующие цели безопасности для ОО, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

**O.SynchrState**

**Обеспечение синхронизации состояния безопасности**

В случае функционирования ОО и других экземпляров ОО, установленных на серверах, для совместного решения задач обеспечения безопасности информации ОО должен обеспечивать возможность проведения надлежащей согласованной синхронизации состояния безопасности, вызванной изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО.

**O.DistrResource**

**Надлежащее распределение ресурсов**

ОО должен обеспечивать для уполномоченного администратора ОО возможность надлежащего распределения дискового и процессорного ресурсов ОО.

**O.FiltrationFlow**

**Фильтрация информационных потоков**

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

В настоящее ЗБ включены следующие функциональные требования безопасности ОО, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

- FDP_IFC.1 «Ограниченное управление информационными потоками»;
- FDP_IFF.1 «Простые атрибуты безопасности»;
- FMT_MSA.1 (3) «Управление атрибутами безопасности»;
- FMT_MSA.1 (4) «Управление атрибутами безопасности»;
- FMT_MSA.3 (2) «Инициализация статических атрибутов»;
- FPT_ITT.1 «Базовая защита внутренней передачи данных ФБО»;
- FPT_SSP.1 «Одностороннее надежное подтверждение»;
- FPT_TRC.1 «Согласованность дублируемых данных ФБО»;
- FPT_FLS.1 «Сбой с сохранением безопасного состояния»;
- FRU_ FLT.2 «Ограниченная отказоустойчивость»;
- FRU_PRS.1 «Ограниченный приоритет обслуживания»;
- FRU_RSA.1 «Максимальные квоты»;
- VDS_VMM.1 (EXT) «Отделение домена виртуальных машин».

# 8 Обоснование

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

## 8.1 Обоснование целей безопасности

### 8.1.1 Обоснование целей безопасности для ОО

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

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

| | O.AccessAssets | O.AccessTOE | O.InteractOS | O.SynchrState | O.AuditEvents | O.ProtectAudit | O.ResidualInform | O.AdminManage | O.ProtectTSF | O.DistrResource | O.TrustedPath | O.FiltrationFlow | O.SafeRecovery | O.TestFunctions | O.SOFAuth |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **T.UnauthAccessData** | X | | | | | | | | | | | | | | |
| **T.UnauthExecProg** | X | | | | | | | | | | | | | | |
| **T.UnauthAccessTOE** | | X | | | | | | | | | | | | | |
| **T.MasqAdmin&User** | | X | | | | | | | | | | | | | |
| **T.UnauthAccessAudit** | | | | | | X | | | | | | | | | |
| **T.LostAudit** | | | | | | X | | | | | | | | | |
| **T.UnauthAccessTSF** | | | | | | | | | X | | | | | | |
| **T.UsageSession** | | X | | | | | | | | | | | | | |
| **T.UnauthUsageRes** | | | | | | | | | | X | | | | | |
| **T.FailureTOE** | | | | | | | | | | | | | X | | |
| **T.FaultConformMng** | | | X | | | | | | | | | | | | |

| | O.AccessAssets | O.AccessTOE | O.InteractOS | O.SynchrState | O.AuditEvents | O.ProtectAudit | O.ResidualInform | O.AdminManage | O.ProtectTSF | O.DistrResource | O.TrustedPath | O.FiltrationFlow | O.SafeRecovery | O.TestFunctions | O.SOFAuth |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **T.FaultConformSrv** | | | | X | | | | | | | | | | | |
| **P.InteractOS** | | | X | | | | | | | | | | | | |
| **P.SynchrState** | | | | X | | | | | | | | | | | |
| **P.AdminManage** | | | | | | | | X | | | | | | | |
| **P.AuditEvents** | | | | | X | | | | | | | | | | |
| **P.AccessAssets** | X | | | | | | | | | | | | | | |
| **P.TrustedPath** | | | | | | | | | | | X | | | | |
| **P.FiltrationFlow** | | | | | | | | | | | | X | | | |
| **P.ResidualInform** | | | | | | | X | | | | | | | | |
| **P.TestFunctions** | | | | | | | | | | | | | | X | |
| **P.SOFAuth** | | | | | | | | | | | | | | | X |

**O.AccessAssets**

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessData, T.UnauthExecProg** и реализацией политики безопасности организации **P.AccessAssets**, так как обеспечивает доступ к защищаемым активам только уполномоченным на это пользователям ОО и администраторам ОО, а также обеспечивает возможность уполномоченным пользователям ОО определять доступность защищаемых активов для других пользователей ОО и администраторов ОО.

**O.AccessTOE**

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessTOE, T.MasqAdmin&User** и **T.UsageSession**, так как обеспечивает доступ к ОО только уполномоченным на это пользователям ОО и администраторам ОО, а также блокирование сеанса пользователя ОО и администратора

ОО, осуществляемое по их инициативе, а также инициируемое ФБО и основанное на интервале времени бездействия пользователя ОО или администратора ОО.

**O.InteractOS**

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.FaultConformMng** и реализацией политики безопасности организации **P.InteractOS**, так как обеспечивает (в случае функционирования ОО, управляемых клиентских и серверных ОС, установленных на рабочих станциях пользователей и отдельных серверах, для совместного решения задач обеспечения безопасности информации) надлежащее согласованное взаимодействие с управляемыми клиентскими и серверными ОС и возможность управления настройками, определяющими ПФБ этих клиентских и серверных ОС.

**O.SynchrState**

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе**T.FaultConformSrv** и реализацией политики безопасности организации **P.SynchrState**, так как обеспечивает (в случае функционирования ОО и других экземпляров ОО, установленных на серверах, для совместного решения задач обеспечения безопасности информации) надлежащую согласованную синхронизацию состояния безопасности, вызванную изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО.

**O.AuditEvents**

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.AuditEvents**, так как обеспечивает наличие надлежащих механизмов регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации предоставляют администраторам ОО возможность выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

**O.ProtectAudit**

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessAudit** и **T.LostAudit**, так как обеспечивает доступ к данным аудита только уполномоченным администраторам ОО и предотвращает потерю данных аудита в случае переполнения их хранилища.

**O.ResidualInform**

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.ResidualInform**, так как обеспечивает недоступность информационного содержания освобождаемой памяти, выделяемой процессам.

**O.AdminManage**

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Manage**, так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования ОО, управляемых клиентских и серверных ОС, доступных только уполномоченным администраторам ОО, а также возможность модификации собственных аутентификационных данных уполномоченными пользователями ОО.

**O.ProtectTSF**

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.UnauthAccessTSF**, так как обеспечивает защиту данных ФБО, поддерживая домен для функционирования ФБО.

**O.DistrResource**

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.UnauthUsageRes**, так как обеспечивает возможность надлежащего распределения дискового и процессорного ресурсов ОО для уполномоченного администратора ОО.

**O.TrustedPath**

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.TrustedPath**, так как обеспечивает невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

**O.FiltrationFlow**

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

**O.SafeRecovery**

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

**O.TestFunctions**

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.TestFunctions**, так как обеспечивает возможность периодического контроля целостности ФБО и его данных, а также возможность собственного регламентного тестирования и тестирования среды функционирования ОО на предмет корректности функционирования.

**O.SOFAuth**

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.SOFAuth**, так как обеспечивает наличие механизма аутентификации, обеспечивающего адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения

### 8.1.2 Обоснование целей безопасности для среды

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

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

| | OE.ImpossibleModif | OE.ConnectTOE | OE.TOEConfig | OE.LocateTOE | OE.NoEvilAdm | OE.NoEvilUser | OE.TrustedLoad | OE.DisableDebugger | OE.SinglePoint | OE.UsagePrint | OE.RegistrDisk | OE.StorageClearing | OE.IntegrityControl | OE.SystemInteraction |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A.ImpossibleModif** | X | | | | | | | | | | | | | |
| **A.ConnectTOE** | | X | | | | | | | | | | | | |
| **A.TOEConfig** | | | X | | | | | | | | | | | |

| | OE.ImpossibleModif | OE.ConnectTOE | OE.TOEConfig | OE.LocateTOE | OE.NoEvilAdm | OE.NoEvilUser | OE.TrustedLoad | OE.DisableDebugger | OE.SinglePoint | OE.UsagePrint | OE.RegistrDisk | OE.StorageClearing | OE.IntegrityControl | OE.SystemInteraction |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A.TrustedLoad** | | | | | | | X | | | | | | | |
| **A.DisableDebugger** | | | | | | | | X | | | | | | |
| **A.UsagePrint** | | | | | | | | | | X | | | | |
| **A.RegistrDisk** | | | | | | | | | | | X | | | |
| **A.StorageClearing** | | | | | | | | | | | | X | | |
| **A.IntegrityControl** | | | | | | | | | | | | | X | |
| **A.LocateTOE** | | | | X | | | | | | | | | | |
| **A.NoEvilAdm** | | | | | X | | | | | | | | | |
| **A.NoEvilUser** | | | | | | X | | | | | | | | |
| **A.SinglePoint** | | | | | | | | | X | | | | | |
| **A.SystemInteraction** | | | | | | | | | | | | | | X |

**OE.ImpossibleModif**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.ImpossibleModif,** так как обеспечивает отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

**OE.ConnectTOE**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.ConnectTOE,** так как обеспечивает осуществление доступа к ОО только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

**OE.TOEConfig**

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

**OE.LocateTOE**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.LocateTOE,** так как обеспечивает, для предотвращения несанкционированного физического доступа, размещение компьютера с установленным ОО в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

**OE.NoEvilAdm**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.NoEvilAdm,** так как обеспечивает прохождение персоналом, ответственным за администрирование ОО, проверок на благонадежность и компетентность, а также деятельность согласно соответствующей документации.

**OE.NoEvilUser**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.NoEvilUser,** так как обеспечивает прохождение уполномоченными на доступ к ОО пользователями проверок на благонадежность, руководство в своей работе эксплуатационной документацией на ОО, совместную деятельность, направленную исключительно на выполнение своих функциональных обязанностей.

**OE.TrustedLoad**

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

**OE.DisableDebugger**

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

**OE.SinglePoint**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.SinglePoint,** так как, при использовании брандмауэра сетевых подключений, обеспечивает, что ОО является единственной точкой доступа в защищаемую внутреннюю вычислительную сеть из внешней вычислительной сети.

**OE.UsagePrint**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.UsagePrint,** так как обеспечивает при осуществлении печати документов регистрацию краткого содержания (наименование, вид, шифр, код) и уровня конфиденциальности выдаваемого на печать документа.

**OE.RegistrDisk**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.RegistrDisk,** так как обеспечивает учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в соответствующий, предусмотренный для этой цели журнал.

**OE.StorageClearing**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.StorageClearing,** так как обеспечивает очистку (обнуление, обезличивание) освобождаемых внешних накопителей путем однократной произвольной записи в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

**OE.IntegrityControl**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.IntegrityControl,** так как обеспечивает надлежащую периодическую поверку целостности программного обеспечения ОО, основанную на проведении контрольного суммирования программного обеспечения ОО.

**OE.SystemInteraction**

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.SystemInteraction,** так как обеспечивает идентификацию взаимодействующих с ОО систем ИТ на основе логических имен.

## 8.2 Обоснование требований безопасности

### 8.2.1 Обоснование требований безопасности для ОО

#### 8.2.1.1 Обоснование функциональных требований безопасности ОО

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

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

| | O.AccessAssets | O.AccessTOE | O.InteractOS | O.SynchrState | O.AuditEvents | O.ProtectAudit | O.ResidualInform | O.AdminManage | O.ProtectTSF | O.DistrResource | O.TrustedPath | O.FiltrationFlow | O.SafeRecovery | O.TestFunctions | O.SOFAuth |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **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 | | | | | | | | | | | | | | |

| | O.AccessAssets | O.AccessTOE | O.InteractOS | O.SynchrState | O.AuditEvents | O.ProtectAudit | O.ResidualInform | O.AdminManage | O.ProtectTSF | O.DistrResource | O.TrustedPath | O.FiltrationFlow | O.SafeRecovery | O.TestFunctions | O.SOFAuth |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FDP_IFC.1 | | | | | | | | | | | | X | | | |
| FDP_IFF.1 | | | | | | | | | | | | X | | | |
| FDP_RIP.1 | | | | | | | X | | | | | | | | |
| FIA_AFL.1 | | X | | | | | | | | | | | | | X |
| FIA_ATD.1 | X | X | | | X | | | X | | | | | | | |
| FIA_SOS.1 | | | | | | | | | | | | | | | X |
| FIA_UAU.2 | X | X | | | | | | | | | | | | | |
| FIA_UAU.7 | | X | | | | | | | | | | | | | |
| FIA_UID.2 | X | X | | | | | | | | | | | | | |
| FIA_USB.1 (EXT) | X | X | | | X | | | | | | | | | | |
| FMT_MOF.1 | | | | | | | | X | | | | | | | |
| FMT_MSA.1 (1) | X | | | | | | | X | | | | | | | |
| FMT_MSA.1 (2) | X | | | | | | | X | | | | | | | |
| FMT_MSA.1 (3) | | | | | | | | X | | | | X | | | |
| FMT_MSA.1 (4) | | | | | | | | X | | | | X | | | |
| FMT_MSA.3 (1) | X | | | | | | | X | | | | | | | |
| FMT_MSA.3 (2) | | | | | | | | X | | | | X | | | |
| FMT_MTD.1 (1) | | | | | | | | X | | | | | | | |
| FMT_MTD.1 (2) | | | | | | | | X | | | | | | | |
| FMT_MTD.2 | | | | | | | | X | | | | | | | |
| FMT_REV.1 (1) | | | | | | | | X | | | | | | | |
| FMT_REV.1 (2) | X | | | | | | | | | | | | | | |
| FMT_SAE.1 | | | | | | | | X | | | | | | | |
| FMT_SMR.1 | X | | | | | X | | X | X | | | | | | |

| | O.AccessAssets | O.AccessTOE | O.InteractOS | O.SynchrState | O.AuditEvents | O.ProtectAudit | O.ResidualInform | O.AdminManage | O.ProtectTSF | O.DistrResource | O.TrustedPath | O.FiltrationFlow | O.SafeRecovery | O.TestFunctions | O.SOFAuth |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FPT_AMT.1 | | | | | | | | | | | | | | X | |
| FPT_FLS.1 | | | | X | | | | | | X | | | X | | |
| FPT_ITT.1 | | | | X | | | | | | | | | | | |
| FPT_RCV.1 | | | | | | | | | | | | | X | | |
| FPT_RVM.1 | | | | | | | | | X | | | | | | |
| FPT_SEP.1 | | | | | | | | | X | | | | | | |
| FPT_SSP.1 | | | | X | | | | | | | | | | | |
| FPT_STM.1 | | | | | X | | | X | | | | | | | |
| FPT_TDC.1 | | | X | | | | | | | | | | | | |
| FPT_TRC.1 | | | | X | | | | | | | | | | | |
| FPT_TST.1 | | | | | | | | | | | | | | X | |
| FRU_FLT.2 | | | | X | | | | | | X | | | X | | |
| FRU_PRS.1 | | | | | | | | | | X | | | | | |
| FRU_RSA.1 | | | | | | | | | | X | | | | | |
| FTA_SSL.1 | | X | | | | | | | | | | | | | |
| FTA_SSL.2 | | X | | | | | | | | | | | | | |
| FTA_TSE.1 | | X | | | | | | | | | | | | | |
| FTP_TRP.1 | | | | | | | | | | | X | | | | |
| VDS_VMM.1. (EXT) | | | | | | | | | X | | | | | | |

**FAU_GEN.1 Генерация данных аудита**

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО.

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

**FAU_GEN.2 Ассоциация идентификатора пользователя**

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

**FAU_SAR.1 Просмотр аудита**

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченному администратору ОО всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

**FAU_SAR.2 Ограниченный просмотр аудита**

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

**FAU_SAR.3 Выборочный просмотр аудита**

Выполнение требований данного компонента обеспечивает выполнение поиска и сортировки данных аудита, основанных на определенных критериях (идентификатор пользователя, тип результата события (успех и/или отказ), источник события, категория события, код события, временной интервал совершения события, идентификатор учетной записи компьютера). Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

**FAU_SEL.1 Избирательный аудит**

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, уполномоченным администратором ОО по таким атрибутам, как идентификатор пользователя, тип результата события (успех и/или отказ), источник события, категория события, код события, временной интервал совершения события, идентификатор учетной

записи компьютера. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

**FAU_STG.1 Защищенное хранение журнала аудита**

Выполнение требований данного компонента обеспечивает защиту хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

**FAU_STG.3 Действия в случае возможной потери данных аудита**

Выполнение требований данного компонента обеспечивает формирование предупреждения уполномоченному администратору ОО, если журнал аудита превысит определенный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

**FAU_STG.4 Предотвращение потери данных аудита**

Выполнение требований данного компонента обеспечивает предотвращение событий, подвергающихся аудиту, и останов ОО при переполнении журнала аудита. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

**FDP_ACC.1 Ограниченное управление доступом**

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

**FDP_IFC.1 Ограниченное управление информационными потоками**

Выполнение требований данного компонента обеспечивает реализацию политики фильтрации информации для субъектов, информации и операций перемещения

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

**FDP_IFF.1 Простые атрибуты безопасности**

Выполнение требований данного компонента обеспечивает осуществление политики фильтрации информации, основываясь на атрибутах безопасности, определении правил фильтрации. Рассматриваемый компонент сопоставлен с целью **O.FiltrationFlow** и способствует ее достижению.

**FDP_RIP.1 Ограниченная защита остаточной информации**

Выполнение требований данного компонента обеспечивает недоступность любого предыдущего информационного содержания памяти при ее освобождении процессами. Рассматриваемый компонент сопоставлен с целью **O.ResidualInformation** и способствует ее достижению.

**FIA_AFL.1 Обработка отказов аутентификации**

Выполнение требований данного компонента обеспечивает ограничение попыток пройти процедуру аутентификации для лиц, не являющихся санкционированными пользователями ОО. При достижении определенного администратором ОО числа неуспешных попыток аутентификации (не более 10) некоторого лица, данное лицо лишается возможности предпринимать дальнейшие попытки пройти процедуру аутентификации. Рассматриваемый компонент сопоставлен с целями **O.AccessTOE, O.SOFAuth** и способствует их достижению.

**FIA_ATD.1 Определение атрибутов пользователя**

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

**FIA_UAU.7 Аутентификация с защищенной обратной связью**

Выполнение требований данного компонента обеспечивает, что во время выполнения аутентификации вводимый пользователем пароль отображается в скрытом виде. Рассматриваемый компонент сопоставлен с целью **O.AccessTOE** и способствует ее достижению.

**FIA_UID.2 Идентификация до любых действий пользователя**

Выполнение требований данного компонента обеспечивает выполнение идентификации **с**убъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целью **O.AccessAssets, O.AccessTOE** и способствует их достижению.

**FIA_USB.1 (EXT) Связывание пользователь-субъект**

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от имени этого субъекта доступа. Рассматриваемый компонент сопоставлен с целями **O.AccessAssets, O.AccessTOE, O.AuditEvents** и способствует их достижению.

**FMT_MOF.1 Управление режимом выполнения функций**

Выполнение требований данного компонента обеспечивает, что ФБО разрешает определенные действия над функциями из числа ФБО только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

**FMT_MSA.1 (1) Управление атрибутами безопасности**

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

**FMT_MSA.1 (2) Управление атрибутами безопасности**

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты управления доступом, ассоциированные с именованным объектом только пользователю ОО, являющемуся владельцем объекта; пользователю ОО, имеющему право смены владельца; пользователю ОО, имеющему право модификации DACL. Рассматриваемый компонент сопоставлен с целями **O.AccessAssets, O.AdminManage** и способствует их достижению.

**FMT_MSA.1 (3) Управление атрибутами безопасности**

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности, используемые в политике фильтрации информации только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.AdminManage, O.FiltrationFlow** и способствует их достижению.

**FMT_MSA.1 (4) Управление атрибутами безопасности**

Выполнение требований данного компонента обеспечивает возможность удалять и создавать атрибуты безопасности для правил управления информационными потоками в политике фильтрации информации только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целями **O.AdminManage, O.FiltrationFlow** и способствует их достижению.

**FMT_MSA.3 (1) Инициализация статических атрибутов**

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для пользователя ОО, являющегося владельцем объекта, определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **O.AccessAssets, O.AdminManage** и способствует их достижению.

**FMT_MSA.3 (2) Инициализация статических атрибутов**

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики фильтрации информации, и возможность для уполномоченного администратора ОО, определять альтернативные значения для отмены значений по

умолчанию. Рассматриваемый компонент сопоставлен с целями **O.AdminManage, O.FiltrationFlow** и способствует их достижению.

**FMT_MTD.1 (1) Управление данными ФБО**

Выполнение требований данного компонента предоставляет возможность осуществлять определенные операции над данными ФБО (см. таблицу 5.4) только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

**FMT_MTD.1 (2) Управление данными ФБО**

Выполнение требований данного компонента предоставляет возможность модификации собственных аутентификационных данных только уполномоченному пользователю ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

**FMT_MTD.2 Управление ограничениями данных ФБО**

Выполнение требований данного компонента предоставляет возможность определения ограничений для порогового значения количества неуспешных попыток аутентификации только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

**FMT_REV.1 (1) Отмена**

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

**FMT_REV.1 (2) Отмена**

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только пользователю ОО, уполномоченному согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта. Рассматриваемый компонент сопоставлен с целью **O.AccessAssets** и способствует ее достижению.

**FMT_SAE.1 Ограниченная по времени авторизация**

Выполнение требований данного компонента предоставляет возможность назначать срок действия для аутентификационных данных только уполномоченному

администратору ОО. По истечении срока действия аутентификационных данных ФБО осуществляют блокирование ассоциированной с пользователем учетной записи. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

**FMT_SMR.1 Роли безопасности**

Данный компонент включен в ЗБ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО. Рассматриваемый компонент сопоставлен с целями **O.AccessAssets, O.ProtectAudit, O.AdminManage, O.ProtectTSF** и способствует их 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 администратора ОО. Рассматриваемый компонент сопоставлен с целью **O.TestFunctions** и способствует ее достижению.

**FPT_FLS.1 Сбой с сохранением безопасного состояния**

Данный компонент включен в ЗБ для того, чтобы обеспечить безопасное функционирование ФБО, в случаях сбоев аппаратных средств. Рассматриваемый компонент сопоставлен с целями **O.SynchrState, O.SafeRecovery, O.DistrResource** и способствует их достижению.

**FPT_ITT.1 Базовая защита внутренней передачи данных ФБО**

Данный компонент включен в ЗБ, для того, чтобы учесть зависимости выполнения требований компонентов FPT_SSP.1 и FPT_TRC.1**.** Выполнение требований данного компонента обеспечивает защиту данных ФБО от раскрытия и модификации при репликации состояния безопасности, проводимой между разными серверами с установленными экземплярами ОО (в случае совместного обеспечения безопасности). Рассматриваемый компонент сопоставлен с целью **O.SynchrState** и способствует ее достижению.

**FPT_RCV.1 Ручное восстановление**

Выполнение требований данного компонента обеспечивает переход ФБО в режим аварийной поддержки для последующего возврата ОО в безопасное состояние после сбоя

или прерывания обслуживания. Рассматриваемый компонент сопоставлен с целью **O.SafeRecovery** 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.ProtectTSF** 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 целью **O.ProtectTSF** и способствует ее достижению.

**FPT_SSP.1 Одностороннее надежное подтверждение**

Выполнение требований данного компонента обеспечивает осуществление репликации состояния безопасности между ФБО и другими экземплярами ОО, установленными на компьютерах, в случае совместного обеспечения безопасности. Рассматриваемый компонент сопоставлен с целью **O.SynchrState** и способствует ее 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 целями **O.AuditEvents, O.AdminManage** и способствует их достижению.

**FPT_TDC.1 Базовая согласованность данных ФБО между ФБО**

Выполнение требований данного компонента обеспечивает надлежащее согласованное взаимодействие ФБО с управляемыми клиентскими и серверными ОС и возможность управления настройками, определяющими ПФБ управляемых клиентских и серверных ОС. Рассматриваемый компонент сопоставлен с целью **O.InteractOS** и способствует ее достижению.

**FPT_TRC.1 Согласованность дублируемых данных ФБО**

Выполнение требований данного компонента обеспечивает согласованность данных ФБО при осуществлении репликации состояния безопасности, проводимой между ФБО и компьютерами с установленными экземплярами ОО (в случае совместного обеспечения безопасности), в том числе и после восстановления состояния доступности компьютеров по отношению к ФБО. Рассматриваемый компонент сопоставлен с целью **O.SynchrState** и способствует ее достижению.

**FPT_TST.1 Тестирование ФБО**

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

**FRU_FLT.2 Ограниченная отказоустойчивость**

Данный компонент включен в ЗБ для того, чтобы обеспечить безопасное функционирование ОО, в случаях сбоев аппаратных средств. Рассматриваемый компонент сопоставлен с целями **O.SynchrState, O.SafeRecovery, O.DistrResource** и способствует их 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.DistrResource** и способствует ее достижению.

**FRU_RSA.1 Максимальные квоты**

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

**FTA_SSL.1 Блокирование сеанса, инициированное ФБО**

Выполнение требований данного компонента обеспечивает блокирование сеанса пользователя ОО или администратора ОО после истечения интервала времени бездействия. Определяются действия, необходимые для разблокирования.

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

**FTA_SSL.2 Блокирование, инициированное пользователем**

Выполнение требований данного компонента обеспечивает блокирование сеанса, инициированное пользователем ОО или администратором ОО. Определяются действия, необходимые для разблокирования. Рассматриваемый компонент сопоставлен с целью **O.AccessTOE** и способствует ее достижению.

**FTA_TSE.1 Открытие сеанса с ОО**

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

**FTP_TRP.1 Доверенный маршрут**

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

**VDS_VMM.1 (EXT) Отделение домена виртуальных машин**

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного функционирования каждой виртуальной машины, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **O.ProtectTSF** и способствует ее достижению.

#### 8.2.1.2 Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ЗБ соответствуют ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), и сформулированы, исходя из соответствия настоящего ЗБ профилю защиты ОС.СОС.ПЗ «Безопасность

информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005».

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

### 8.2.2 Обоснование зависимостей требований

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

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

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

Таблица 8.4 – Зависимости функциональных требований

| Функциональные компоненты | Зависимости по ОК | Удовлетворение зависимостей |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 |
| FAU_GEN.2 | FAU_GEN.1,<br>FIA_UID.1 | FAU_GEN.1,<br>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,<br>FMT_MTD.1 | FAU_GEN.1,<br>FMT_MTD.1 (1) |

| Функциональные компоненты | Зависимости по ОК | Удовлетворение зависимостей |
|---|---|---|
| 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,<br>FMT_MSA.3 | FDP_ACC.1,<br>FMT_MSA.3 (1) |
| FDP_IFC.1 | FDP_IFF.1 | FDP_IFF.1 |
| FDP_IFF.1 | FDP_IFC.1,<br>FMT_MSA.3 | FDP_IFC.1,<br>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 (EXT) | FIA_ATD.1 | FIA_ATD.1 |
| FMT_MOF.1 | FMT_SMR.1 | FMT_SMR.1 |
| FMT_MSA.1 (1) | [FDP_ACC.1 или<br>FDP_IFC.1],<br>FMT_SMR.1 | FDP_ACC.1,<br>FMT_SMR.1 |
| FMT_MSA.1 (2) | [FDP_ACC.1 или<br>FDP_IFC.1],<br>FMT_SMR.1 | FDP_ACC.1,<br>FMT_SMR.1 |
| FMT_MSA.1 (3) | [FDP_ACC.1 или<br>FDP_IFC.1],<br>FMT_SMR.1 | FDP_IFC.1,<br>FMT_SMR.1 |
| FMT_MSA.1 (4) | [FDP_ACC.1 или<br>FDP_IFC.1],<br>FMT_SMR.1 | FDP_IFC.1,<br>FMT_SMR.1 |
| FMT_MSA.3 (1) | FMT_MSA.1,<br>FMT_SMR.1 | FMT_MSA.1 (1),<br>FMT_MSA.1 (2), |

| Функциональные компоненты | Зависимости по ОК | Удовлетворение зависимостей |
|---|---|---|
| | | FMT_SMR.1 |
| FMT_MSA.3 (2) | FMT_MSA.1,<br>FMT_SMR.1 | FMT_MSA.1 (3),<br>FMT_MSA.1 (4),<br>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.2 | FMT_MTD.1,<br>FMT_SMR.1 | FMT_MTD.1 (1),<br>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,<br>FPT_STM.1 | FMT_SMR.1,<br>FPT_STM.1 |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.2 |
| FPT_RCV.1 | FPT_TST.1,<br>AGD_ADM.1,<br>ADV_SPM.1 | FPT_TST.1,<br>AGD_ADM.1,<br>*обосновано невключение ADV_SPM.1* |
| FPT_FLS.1 | ADV_SPM.1 | *обосновано невключение ADV_SPM.1* |
| FPT_SSP.1 | FPT_ITT.1 | FPT_ITT.1 |
| FPT_TRC.1 | FPT_ITT.1 | FPT_ITT.1 |
| FPT_TST.1 | FPT_AMT.1 | FPT_AMT.1 |
| FPT_FLS.1 | FPT_FLS.1 | FPT_FLS.1 |
| FTA_SSL.1 | FIA_UAU.1 | FIA_UAU.2 |
| FTA_SSL.2 | FIA_UAU.1 | FIA_UAU.2 |
| AVA_SOF.1 | ADV_FSP.1,<br>ADV_HLD.1 | ADV_FSP.1,<br>*обосновано невключение* ADV_HLD.1 |

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

Включение в ЗБ компонента AVA_SOF.1 требует для удовлетворения зависимостей включения компонента ADV_HLD.1, разработчиком в функциональной спецификации описан механизм идентификации, используемый ОО. В связи с этим зависимость компонента AVA_SOF.1 от компонента ADV_HLD.1 не учитывается.

Все остальные зависимости включенных в ЗБ функциональных компонентов удовлетворены.

## 8.3 Обоснование краткой спецификации ОО

Обоснование краткой спецификации ОО представлено таблицей 8.5 и таблицей 8.6.

Таблица 8.5 – Отображение функциональных требований безопасности на функции безопасности.

| | **Аудит безопасности** | **Защита данных пользователя** | **Идентификация и аутентификация** | **Управление безопасностью** | **Защита ФБО** | **Использование ресурсов ОО** | **Блокирование сеанса** | **Управление доступом к ОО** |
|---|---|---|---|---|---|---|---|---|
| **FAU_GEN.1** | **X** | | | | | | | |

| | Аудит безопасности | Защита данных пользователя | Идентификация и аутентификация | Управление безопасностью | Защита ФБО | Использование ресурсов ОО | Блокирование сеанса | Управление доступом к ОО |
|---|---|---|---|---|---|---|---|---|
| FAU_GEN.2 | X | | | | | | | |
| FAU_SAR.1 | X | | | | | | | |
| FAU_SAR.2 | X | | | | | | | |
| FAU_SAR.3 | X | | | | | | | |
| FAU_SEL.1 | X | | | | | | | |
| FAU_STG.1 | X | | | | | | | |
| FAU_STG.3 | X | | | | | | | |
| FAU_STG.4 | X | | | | | | | |
| FDP_ACC.1 | | X | | | | | | |
| FDP_ACF.1 | | X | | | | | | |
| FDP_IFC.1 | | X | | | | | | |
| FDP_IFF.1 | | X | | | | | | |
| FDP_RIP.1 | | X | | | | | | |
| FIA_AFL.1 | | | X | | | | | |
| FIA_ATD.1 | | | X | | | | | |
| FIA_SOS.1 | | | X | | | | | |
| FIA_UAU.2 | | | X | | | | | |
| FIA_UAU.7 | | | X | | | | | |
| FIA_UID.2 | | | X | | | | | |

| | Аудит безопасности | Защита данных пользователя | Идентификация и аутентификация | Управление безопасностью | Защита ФБО | Использование ресурсов ОО | Блокирование сеанса | Управление доступом к ОО |
|---|---|---|---|---|---|---|---|---|
| FIA_USB.1 (EXT) | | | X | | | | | |
| FMT_MOF.1 | | | | X | | | | |
| FMT_MSA.1 (1) | | | | X | | | | |
| FMT_MSA.1 (2) | | | | X | | | | |
| FMT_MSA.1 (3) | | | | X | | | | |
| FMT_MSA.1 (4) | | | | X | | | | |
| FMT_MSA.3 (1) | | | | X | | | | |
| FMT_MSA.3 (2) | | | | X | | | | |
| FMT_MTD.1 (1) | | | | X | | | | |
| FMT_MTD.1 (2) | | | | X | | | | |
| FMT_MTD.2 | | | | X | | | | |
| FMT_REV.1 (1) | | | | X | | | | |
| FMT_REV.1 (2) | | | | X | | | | |
| FMT_SAE.1 | | | | X | | | | |
| FMT_SMR.1 | | | | X | | | | |
| FPT_AMT.1 | | | | | X | | | |
| FPT_FLS.1 | | | | | X | | | |
| FPT_ITT.1 | | | | | X | | | |
| FPT_RCV.1 | | | | | X | | | |

| | Аудит безопасности | Защита данных пользователя | Идентификация и аутентификация | Управление безопасностью | Защита ФБО | Использование ресурсов ОО | Блокирование сеанса | Управление доступом к ОО |
|---|---|---|---|---|---|---|---|---|
| FPT_RVM.1 | | | | | X | | | |
| FPT_SEP.1 | | | | | X | | | |
| FPT_SSP.1 | | | | | X | | | |
| FPT_STM.1 | | | | | X | | | |
| FPT_TDC.1 | | | | | X | | | |
| FPT_TRC.1 | | | | | X | | | |
| FPT_TST.1 | | | | | X | | | |
| FRU_FLT.2 | | | | | | X | | |
| FRU_PRS.1 | | | | | | X | | |
| FRU_RSA.1 | | | | | | X | | |
| FTA_SSL.1 | | | | | | | X | |
| FTA_SSL.2 | | | | | | | X | |
| FTA_TSE.1 | | | | | | | | X |
| FTP_TRP.1 | | | X | | | | | |
| VDS_VMM.1 (EXT) | | | | | X | | | |

Таблица 8.6 – Отображение требований доверия на меры безопасности.

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

## 8.4 Обоснование требований к стойкости функций безопасности

Термин «стойкость функции» определен в части 1 ОК как характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного режима при прямой атаке на лежащие в ее основе механизмы безопасности. В части 1 ОК определено три уровня стойкости функции: базовая СФБ, средняя СФБ и высокая СФБ. В настоящем ЗБ выбран уровень стойкости функции – средняя СФБ. Средняя СФБ – это уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения. Выбор СФБ в ЗБ определялся, исходя из возможностей ОО и обеспечения соответствия ОО профилю защиты ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005». Выбор средней СФБ в качестве минимального уровня

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

## 8.5 Обоснование утверждений о соответствии ПЗ

Объект оценки соответствует профилю защиты ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

### 8.5.1 Обоснование конкретизации требований безопасности ИТ

Все требования безопасности, сформулированные в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Операции подобных требований завершены в настоящем ЗБ в полном объеме.

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

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

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

### 8.5.2 Обоснование добавления угроз безопасности

В настоящее ЗБ включены следующие угрозы, которым противостоит ОО, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

**T.FaultConformSrv** – включена в связи с возможностью ОО, связанной с противостоянием нарушениям режимов взаимодействия ОО и других экземпляров ОО, установленных на серверах для решения задач совместного с ОО обеспечения безопасности информации, вследствие несогласованной интерпретации совместно используемых данных ФБО.

**T.UnauthUsageRes** – включена в связи с возможностью ОО, связанной с противостоянием исчерпанию свободных ресурсов ОО (вычислительные возможности, дисковое пространство) вследствие неограниченного их использования пользователями ОО.

### 8.5.3 Обоснование добавления политик безопасности организации

В настоящее ЗБ включены следующие политики безопасности организации, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

**P.SynchrState** – включена в связи с возможностью ОО, связанной с проведением надлежащей синхронизации состояния безопасности, вызванной изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО, в случае функционирования ОО и других экземпляров ОО, установленных на серверах, для совместного решения задач обеспечения безопасности информации и управления клиентскими и серверными ОС.

**P.FiltrationFlow** – включена в связи с возможностью ОО, связанной с осуществлением фильтрации входящих в ОО информационных потоков.

### 8.5.4 Обоснование добавления целей безопасности для ОО

В настоящее ЗБ включена следующие цели безопасности для ОО, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

**O.SynchrState** – в случае функционирования ОО и других экземпляров ОО, установленных на серверах, для совместного решения задач обеспечения безопасности информации, ОО должен обеспечивать возможность проведения надлежащей согласованной синхронизации состояния безопасности, вызванной изменениями безопасности, произведенными как на ОО, так и на других экземплярах ОО.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ политики безопасности организации **P.SynchrState** и необходимостью ее реализации, а также добавлением в ЗБ угрозы безопасности **T.FaultConformSrv** и необходимостью противостояния ей.

**O.DistrResource –** ОО должен обеспечивать для уполномоченного администратора ОО возможность надлежащего распределения дискового и процессорного ресурсов ОО.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ угрозы безопасности **T.UnauthUsageRes** и необходимостью противостояния ей.

**O.FiltrationFlow –** ОО должен располагать механизмами, осуществляющими фильтрацию входящих в ОО информационных потоков.

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

### 8.5.5 Обоснование добавления требований безопасности ИТ

В настоящее ЗБ включены следующие функциональные требования безопасности ОО, не вошедшие в ПЗ ОС.СОС.ПЗ «Безопасность информационных технологий. Операционные системы. Серверные операционные системы. Профиль защиты. Версия 1.0, 2005»:

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

Компонент функциональных требований безопасности FDP_IFF.1 – включен в связи с возможностью ОО осуществлять фильтрацию входящих информационных потоков по определенным правилам, с использованием определенных атрибутов и в соответствии с политикой фильтрацией информации.

Компонент функциональных требований безопасности FMT_MSA.1 (3) – включен в связи с возможностью ОО, связанной с модификацией атрибутов безопасности, используемых в политике фильтрации информации, которая предоставляется только уполномоченному администратору ОО.

Компонент функциональных требований безопасности FMT_MSA.1 (4) – включен в связи с возможностью ОО, связанной с удалением и созданием атрибутов безопасности для правил политики фильтрации информации.

Компонент функциональных требований безопасности FMT_MSA.3 (2) – включен в связи с возможностью ОО, связанной с использованием ограничительных значений по умолчанию для атрибутов безопасности, которые используются для осуществления политики фильтрации информации, а также возможностью уполномоченного администратора ОО изменять значения по умолчанию для указанных атрибутов безопасности.

Компонент функциональных требований безопасности FPT_FLS.1 – включен в связи с возможностью ОО сохранять режим безопасного функционирования ФБОв случае аппаратных сбоев.

Компонент функциональных требований безопасности FPT_ITT.1 – включен в связи с возможностью ОО защищать данные ФБО от раскрытия и модификации при репликации состояния безопасности, проводимой между разными серверами с установленными экземплярами ОО (в случае совместного обеспечения безопасности).

Компонент функциональных требований безопасности FPT_SSP.1 – включен в связи с возможностью ОО осуществлять репликацию состояния безопасности с другими экземплярами ОО.

Компонент функциональных требований безопасности FPT_TRC.1 – включен в связи с возможностью ОО обеспечивать согласованность данных ФБО при репликации состояния безопасности, проводимой между ФБО и серверам с установленными экземплярами ОО (в случае совместного обеспечения безопасности).

Компонент функциональных требований безопасности FRU_FLT.2 – включен в связи с возможностью ОО сохранять режима безопасного функционирования в случае аппаратных сбоев.

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

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

Компонент функциональных требований безопасности VDS_VMM.1 (EXT) – сформулирован в явном виде. Введение данного компонента, было вызвано использованием особого механизма безопасности для реализации ФБ «Защита ФБО». Для

создания виртуальных машин ОО создается домен безопасности, в котором функционирует каждая виртуальная машина. Домены безопасности обеспечивают защиту безопасного функционирования ФБО для каждой виртуальной машины.