СОГЛАСОВАНО
НАЧАЛЬНИК УПРАВЛЕНИЯ
ФСТЭК РОССИИ

В.СЕЛИН
« »_____ 2006 ГОДА

УТВЕРЖДАЮ
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
ООО «МАЙКРОСОФТ РУС»

Б.СТЕЕН
« »_____ 2006 ГОДА

MICROSOFT® INTERNET SECURITY AND ACCELERATION SERVER™ 2006

ЗАДАНИЕ ПО БЕЗОПАСНОСТИ

MS.ISA_SRV2006_STD.ЗБ

Версия 1.0

2006

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АИС	– автоматизированная информационная система
ЗБ	– задание по безопасности
ИТ	– информационная технология
МЭ	– межсетевой экран
НСД	– несанкционированный доступ
ОДФ	– область действия функции безопасности объекта оценки
ОК	– Общие критерии
ОО	– объект оценки
ОС	– операционная система
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
СФБ	– стойкость функции безопасности
ФБ	– функция безопасности
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональные требования безопасности
API	– Application Programming Interface
IRC	– Internet Relay Chat
IP	– Internet Protocol
ISA	– Internet Security and Acceleration
MIME	– Multipurpose Internet Mail Extensions
MMC	– Microsoft Management Console
MMS	– Microsoft Media Streaming
MSDE	– Microsoft Database Engine
NAT	– Network Address Translation
OSI	– Open System Interconnection
PNM	– RealNetworks Streaming Media Protocol
RPC	– Remote Procedure Call
RTSP	– Real Time Streaming Protocol
SSL	– Secure Socket Layer
VPN	– Virtual Private Network

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:	Microsoft® Internet Security and Acceleration Server™ 2006 Standard Edition. Задание по безопасности.
Версия ЗБ:	Версия 1.0.
Обозначение ЗБ:	MS.ISA_Srv2006_Std.ЗБ.
Идентификация ОО:	Программный комплекс Microsoft® Internet Security and Acceleration Server™ 2006 Standard 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. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, ФСТЭК (Гостехкомиссия) России, 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, ФСТЭК (Гостехкомиссия)

России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, ФСТЭК (Гостехкомиссия) России, 2002.

Ключевые слова: Межсетевой экран, средство защиты информации, задание по безопасности, ОУД1, Microsoft®.

1.2 Аннотация ЗБ

Настоящее ЗБ определяет требования безопасности для программного комплекса Microsoft® Internet Security and Acceleration Server™ 2006 Standard Edition.

Программный комплекс Microsoft® Internet Security and Acceleration Server™ 2006 Standard Edition – программный межсетевой экран, предназначенный для защиты информационных систем организаций от внутренних и внешних атак и контроля доступа между компьютерами внутренней и внешней сети.

1.3 Соответствие ОК

Объект оценки и ЗБ согласованы со следующими спецификациями:

- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, ФСТЭК (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, ФСТЭК (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);
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели

защищенности от несанкционированного доступа к информации. ФСТЭК (Гостехкомиссия) России, 1997 (**соответствие 3 классу защищенности**).

1.4 Соглашения

Руководящий документ ФСТЭК (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 включены компоненты функциональных требований безопасности, сформулированные в явном виде. Краткая форма имени функциональных компонентов, сформулированных 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 при регистрации.

Данные пользователя – данные, созданные пользователем и для пользователя, которые не влияют на выполнение ФБО.

Достоверность – свойство безопасности активов, обеспечивающее соответствие предусмотренным значениям.

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

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО (в данном случае – программного комплекса Microsoft® Internet Security and Acceleration Server™ 2006 Standard Edition).

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

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

Объект оценки – подлежащий оценке программный комплекс Microsoft® Internet Security and Acceleration Server™ 2006 Standard Edition с руководствами по эксплуатации.

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

Политика функции безопасности – политика безопасности, осуществляемая ФБ.

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

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 (в данном случае продукт ИТ совпадает с ОО, идентифицированным в настоящем ЗБ).

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

1.6 Организация ЗБ

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

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

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

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

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 ОК определены, соответственно, функциональные требования безопасности ИТ (для ОО и его среды функционирования) 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» указано, что в ЗБ нет утверждений о соответствии ОО какому-либо профилю защиты.

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 программный комплекс Microsoft® Internet Security and Acceleration Server™ 2006 Standard Edition (далее – межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition).

Объект оценки предназначен для использования в автоматизированных системах класса защищенности до 1Г включительно.

2.1 Тип продукта ИТ

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition (ISA Server™) предназначен для защиты автоматизированных информационных систем и сетей организаций от внутренних и внешних атак и для оптимизации информационного трафика при работе с данными. Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition совмещает в себе следующие роли:

- трехуровневого фильтрующего межсетевого экрана;
- веб-прокси сервера;
- VPN-сервера или VPN-шлюза.

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition можно настроить для работы в каждой из этих ролей или набора этих ролей.

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition обеспечивает контроль входящего и исходящего информационного потока посредством трехуровневой фильтрации, необходимой для защиты сетей: фильтрации уровня пакетов, фильтрации уровня канала и фильтрации уровня приложения.

2.2 Основные функциональные возможности продукта ИТ

В межсетевом экране Microsoft® ISA Server™ 2006 Standard Edition реализован ряд функциональных возможностей по**:**

- обеспечению безопасности;
- высокопроизводительному веб-кэшированию;
- управлению;
- расширяемости.

В данном подразделе представлено краткое описание этих функциональных возможностей.

2.2.1 Основные функциональные возможности по обеспечению безопасности

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition обеспечивает защиту АИС организации от внутренних и внешних атак, а также контроль и безопасность доступа между компьютерами внутренней и внешней сетей посредством функциональных возможностей по обеспечению безопасности.

2.2.1.1 Многоуровневый межсетевой экран

Для достижения максимального уровня безопасности АИС организации в межсетевом экране Microsoft® ISA Server™ 2006 Standard Edition реализована трехуровневая фильтрация: фильтрация пакетов, фильтрация уровня канала и фильтрация потока данных приложений. На рисунке 2.1 показана связь уровней фильтрации с сетевой моделью OSI (эталонной моделью взаимодействия открытых сетей).

Рисунок 2.1 – Взаимосвязь уровней фильтрации и сетевой модели OSI

Фильтрация пакетов

Фильтрация пакетов осуществляется на сетевом уровне модели OSI. При этом анализируются заголовки пакетов, содержащие IP-адреса и свойства пакета, и блокируется или пропускается трафик через межсетевой экран на основе полученной информации.

Microsoft® ISA Server™ 2006 Standard Edition использует технологию динамической фильтрации пакетов. По мере необходимости автоматически выполняется открытие, а по завершении сеанса связи – закрытие соответствующих портов.

Фильтрация уровня канала

Фильтрация уровня канала осуществляется на транспортном и сеансовом уровнях модели OSI. При этом исследуется информация квитирования протокола TCP, пересылаемая между компьютерами, для определения легитимности сеансового запроса. Фильтрация уровня канала позволяет администраторам ОО анализировать сеансы. Сеанс рассматривается как аналог соединения, но в действительности сеанс может состоять более чем из одного соединения. Сеансы устанавливаются только в ответ на запрос пользователя, что обеспечивает дополнительную безопасность.

Фильтрация каналов обеспечивает прозрачный для приложений шлюз для межплатформенного доступа к Telnet, RealAudio, Windows Media, IRC, а также ко многим другим протоколам и службам. В Microsoft® ISA Server™ 2006 Standard Edition фильтрация каналов осуществляется совместно с динамической фильтрацией пакетов, что упрощает ее использование и повышает общую безопасность работы сети.

Фильтры уровня канала не ограничивают доступ, основываясь на информации о пользователе; они также не могут распознавать команды протоколов. Для этого используется фильтрация уровня приложения.

Фильтрация уровня приложения

Фильтрация уровня приложения работает на верхнем уровне сетевой модели OSI – уровне приложения. Фильтры уровня приложения могут использовать информацию из заголовка пакета, а также содержимого потока данных и информации о пользователе.

Администраторы ОО могут использовать фильтрацию уровня приложения для контроля доступа на основе идентичности пользователя и/или на основе конкретной задачи, которую пытается осуществить пользователь.

На основе анализа содержания потока данных можно пропускать, блокировать, перенаправлять или изменять данные протоколов HTTP, FTP, SMTP, POP3, DNS, данных конференций по протоколу H.323, потокового мультимедиа, удаленного вызова процедур и VPN.

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition имперсонирует во внутренней сети клиентские компьютеры, скрывая от внешней среды внутреннюю топологию сети и IP-адреса предприятия.

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition использует динамическую проверку данных на уровне приложений. Во избежание возможных разрывов подключения или нарушения системы безопасности это делается с учетом контекста данных приложения и состояния подключения.

2.2.1.2 Контроль доступа с помощью политик

В межсетевом экране Microsoft® ISA Server™ 2006 Standard Edition можно контролировать входящий и исходящий доступ по:

- пользователям;
- группам;
- используемым приложениям;
- источнику и месту назначения,
- изменению контента,
- расписанию.

С помощью мастеров политик межсетевого экрана определяются доступные веб-узлы и содержание, доступность определенного протокола для установки входящих и исходящих подключений, а также разрешения на установку подключений между определенными IP-адресами с помощью заданных протоколов и портов.

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition поддерживает ряд протоколов, в том числе HTTP/SSL, FTP, RDP, Telnet, RealAudio и RealVideo, IRC, H.323, потоковое мультимедиа, почтовые и новостные протоколы.

2.2.1.3 Безопасная публикация

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition позволяет безопасно публиковать веб-серверы, почтовые серверы и приложения электронной торговли. Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition способен выступать посредником между опубликованным сервером и внешними пользователями, реализуя дополнительный уровень защиты. Для защиты внутренних серверов в правилах веб-публикации можно определить доступные компьютеры, а правила публикации средств управления сервером защищают внутренние серверы от незаконного доступа со

стороны внешних пользователей. Кроме того, опубликованные серверы защищены от атак извне с помощью интеллектуальной фильтрации данных приложений.

2.2.1.4 Обнаружение вторжений

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition Microsoft® ISA Server™ 2006 Standard Edition имеет систему обнаружения и предотвращения наиболее распространенных форм сетевых вторжений. Данная система способна распознавать попытки атаки определенного типа, уведомлять администратора ОО и выполнять заранее заданные действия.

2.2.1.5 Встроенная поддержка VPN

Для предоставления стандартного безопасного удаленного доступа используются встроенные службы виртуальных частных сетей Microsoft® Windows® 2000 и Microsoft® Windows® Server 2003. Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition поддерживает безопасные VPN-подключения филиалов или удаленных пользователей к основному офису. Политика межсетевого экрана применяется к VPN-подключениям и позволяет точно контролировать протоколы и ресурсы, к которым получают доступ пользователи таких подключений.

Одно из главных преимуществ применения VPN-соединения по сравнению с клиент-серверным веб-приложением заключается в том, что удаленные VPN-пользователи, могут получить доступ ко всем протоколам и серверам корпоративной сети.

2.2.1.6 Проверка подлинности пользователей

Проверка подлинности пользователей может проводиться по данным локальной базы данных SAM на межсетевом экране, базы данных Active Directory или с помощью службы RADIUS.

Для клиентов веб-прокси и межсетевого экрана Microsoft® ISA Server™ 2006 Standard Edition поддерживает аутентификацию Windows (NTLM и Kerberos). Для клиентов веб-прокси поддерживаются клиентские сертификаты, выборочная, базовая, анонимная проверка подлинности, а также проверка подлинности на основе форм.

2.2.2 Высокопроизводительное веб-кэширование

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition позволяет снижать загрузку полосы пропускания посредством функциональных возможностей веб-кэширования.

2.2.2.1 Высокопроизводительное прямое и обратное веб-кэширование

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition обеспечивает два типа высокопроизводительного кэширования:

- прямое кэширование – используется для внутренних клиентов, получающих доступ к серверам внешних сетей;
- обратное кэширование – используется для внешних пользователей, получающих доступ ко внутреннему веб-серверу.

Для достижения максимальной производительности используется быстрое кэширование в оперативной памяти и оптимизированный дисковый кэш.

2.2.2.2 Интеллектуальное кэширование

Активное кэширование часто используемых объектов гарантирует их регулярное обновление для каждого пользователя межсетевого экрана. Microsoft® ISA Server™ 2006 Standard Edition автоматически определяет часто используемые веб-сайты, а также необходимую частоту обновления их содержания (на основании продолжительности пребывания объекта в кэше или времени последнего извлечения объекта). В периоды низкого потребления сетевых ресурсов межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition без вмешательства диспетчера сети предварительно загружает веб-контент в кэш. Кроме того, веб-кэш межсетевого экрана Microsoft® ISA Server™ 2006 Standard Edition можно использовать для предварительной загрузки автономного контента, который хранится на компакт- или DVD-дисках.

2.2.2.3 Кэширование по расписанию

В межсетевом экране Microsoft® ISA Server™ 2006 Standard Edition имеется возможность предварительной загрузки в кэш целых веб-сайтов по определенному расписанию. За счет этого можно предоставить пользователям на предприятии доступ к контенту на автономных веб-серверах.

2.2.3 Управление

Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition обеспечивает удобные средства управления для выполнения стандартных задач.

2.2.3.1 Упрощенное управление

В межсетевом экране Microsoft® ISA Server™ 2006 Standard Edition имеются интуитивно понятная графическая панель задач и мастера конфигурации, упрощающие навигацию и настройку стандартных задач. С помощью мастера можно выполнять безопасную публикацию веб-серверов и серверов приложений во внешние сети, настраивать межсетевой экран на выполнение функций сервера или шлюза VPN и создавать правила межсетевого экрана.

Конфигурацию межсетевого экрана можно целиком скопировать в файл XML. Затем такой файл переносится на сменный носитель или отправляется в составе безопасного почтового сообщения администратору другого межсетевого экрана, чтобы обеспечить стандартную конфигурацию в рамках всей организации. Кроме того, из XML файла можно импортировать отдельные элементы конфигурации.

2.2.3.2 Удаленное управление

Удаленное управление межсетевым экраном Microsoft® ISA Server™ 2006 Standard Edition возможно посредством:

- оснастки MMC;
- служб терминалов Windows 2000;
- удаленного рабочего стола Windows Server 2003.

Для удаленного управления межсетевым экраном на компьютере с операционной системой Microsoft® Windows® Server 2003 может использоваться безопасное туннелирование SSL/RDP. Кроме того, удаленное управление службами межсетевого экрана Microsoft® ISA Server™ 2006 Standard Edition возможно с помощью сценариев, запускаемых из командной строки.

2.2.3.3 Журналы, отчеты и оповещения

В межсетевом экране Microsoft® ISA Server™ 2006 Standard Edition журналы безопасности и доступа могут создаваться в:

- текстовом файле с символами-разделителями;

- базе данных SQL;
- базе данных MSDE.

Кроме того, есть возможность создавать по определенному графику стандартные отчеты об использовании сети и приложений, моделях потока сетевых данных и безопасности с автоматической публикацией на локальном или удаленном ресурсе.

Оповещения на основе событий служат для отправки сообщений администратору ОО, запуска и остановки служб межсетевого экрана, а также автоматического выполнения действий на основании заданных критериев.

2.2.4 Расширяемая платформа

Независимые разработчики предлагают программы (например, антивирусное ПО, средства управления, фильтрации содержания и составления отчетов), предназначенные для использования с межсетевым экраном Microsoft® ISA Server™ 2006 Standard Edition, с учетом особенностей продукта. Существуют фильтры сторонних разработчиков, с помощью которых можно предотвратить загрузку в защищенную сеть предприятия последних версий вирусов, сценариев Java и элементов управления ActiveX.

В состав межсетевого экрана Microsoft® ISA Server™ 2006 Standard Edition включены подробные файлы справки Software Development Kit по разработке средств на основе функций межсетевого экрана, кэширования и управления продуктом, а также полная документация API и примеры создания дополнительных веб-фильтров и фильтров приложений, оснасток MMC, средств составления отчетов, сценариев, оповещений и других средств.

2.3 Среда функционирования и границы ОО

2.3.1 Варианты функционирования ОО

При установке и конфигурировании межсетевого экрана Microsoft® ISA Server™ 2006 Standard Edition возможно конфигурировать сетевые правила и политики внутреннего и внешнего доступа вручную или использовать сетевые шаблоны для облегчения процесса конфигурирования. При использовании сетевых шаблонов создаются сети, устанавливаются отношения маршрутизации между сетями с помощью сетевых правил, а затем создаются подробные политики внутреннего и внешнего доступа.

В межсетевом экране Microsoft® ISA Server™ 2006 Standard Edition предусмотрена возможность использования сетевых шаблонов для облегчения процесса конфигурирования сетевых правил и политик внутреннего и внешнего доступа. Эти шаблоны включают следующие наиболее распространенные схемы сетей:

- пограничный межсетевой экран;
- трехзонная конфигурация сервера;
- внешний межсетевой экран;
- внутренний межсетевой экран;
- одна сетевая плата.

Выбор сетевого шаблона определяется используемой в организации схемой сети.

Шаблон пограничного межсетевого экрана

Шаблон пограничного межсетевого экрана используется для подключения внутренней сети к внешним сетям и защиты внутренней сети от несанкционированного доступа. Шаблон пограничного межсетевого экрана применяется, если межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition находится на границе корпоративной сети с внешней сетью.

Шаблон пограничного межсетевого экрана предполагает наличие хотя бы двух сетевых интерфейсов, подключенных:

- к внешней сети;
- к внутренней сети.

Шаблон трехзонной конфигурации сервера

Шаблон трехзонной конфигурации сервера используется для подключения внутренней сети к внешней сети, защиты внутренней сети от несанкционированного доступа, а также для публикации служб во внешней сети из демилитаризованной зоны.

Данный шаблон предполагает наличие хотя бы трех сетевых интерфейсов, подключенных:

- к внешней сети;
- к внутренней сети.
- к сети демилитаризованной зоны.

Шаблон внешнего межсетевого экрана

Шаблон внешнего межсетевого экрана используется, если имеется два межсетевых экрана между защищенной внутренней сетью и внешней сетью. Межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition используется как передняя линия защиты в конфигурации демилитаризованной зоны с двумя межсетевыми экранами. При этом межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition считается внешним, а межсетевой экран, расположенный позади него, – внутренним.

Шаблон внешнего межсетевого экран предполагает наличие хотя бы двух сетевых интерфейсов, подключенных:

- к внешней сети;
- к сети демилитаризованной зоны.

Шаблон внутреннего межсетевого экрана

Шаблон внутреннего межсетевого экрана используется, если имеется два межсетевых экрана между защищенной внутренней сетью и внешней сетью. Microsoft® ISA Server™ 2006 Standard Edition используется как внутренняя линия защиты в конфигурации демилитаризованной зоны с двумя межсетевыми экранам. При этом межсетевой экран Microsoft® ISA Server™ 2006 Standard Edition считается внутренним, а межсетевой экран, расположенный впереди него, – внешним.

Шаблон внутреннего межсетевого экран предполагает наличие хотя бы двух сетевых интерфейсов, подключенных:

- к сети демилитаризованной зоны
- к внутренней сети.

Шаблон с одной сетевой платой

Шаблон с одной сетевой платой используется внутри внутренней сети или демилитаризованной зоны, если Microsoft® ISA Server™ 2006 Standard Edition будет использоваться для веб-прокси, кэширования, веб-публикации или публикации сервера веб-клиента Outlook.

Данный шаблон предполагает наличие хотя бы одного сетевого интерфейса, подключенного к внутренней сети или сети демилитаризованной зоны.

2.3.2 Логические границы ОО

Объект оценки функционирует под управлением операционной системы Microsoft® Windows® Server 2003 (минимально необходимый пакет обновления – SP1).

Объект оценки позволяет устанавливать защищенное соединение с внешними сетями. Для достижения максимального уровня безопасности при межсетевом взаимодействии используется фильтрация пакетов, фильтрация уровня канала и фильтрация потока данных приложений. ОО может также выполнять динамическую фильтрацию, открывая порты взаимодействия только по запросу пользователей, и закрывать их впоследствии.

На рисунке 2.2 представлены основные службы безопасности ОО, реализующие оцениваемые (в соответствии с настоящим ЗБ) функции безопасности ОО, а также компоненты и функциональные возможности межсетевого экрана Microsoft® ISA Server™ 2006 Standard Edition и Microsoft® Windows® Server 2003 и логические связи между ними (показаны стрелками). Направления стрелок указывают направление возможных информационных потоков.

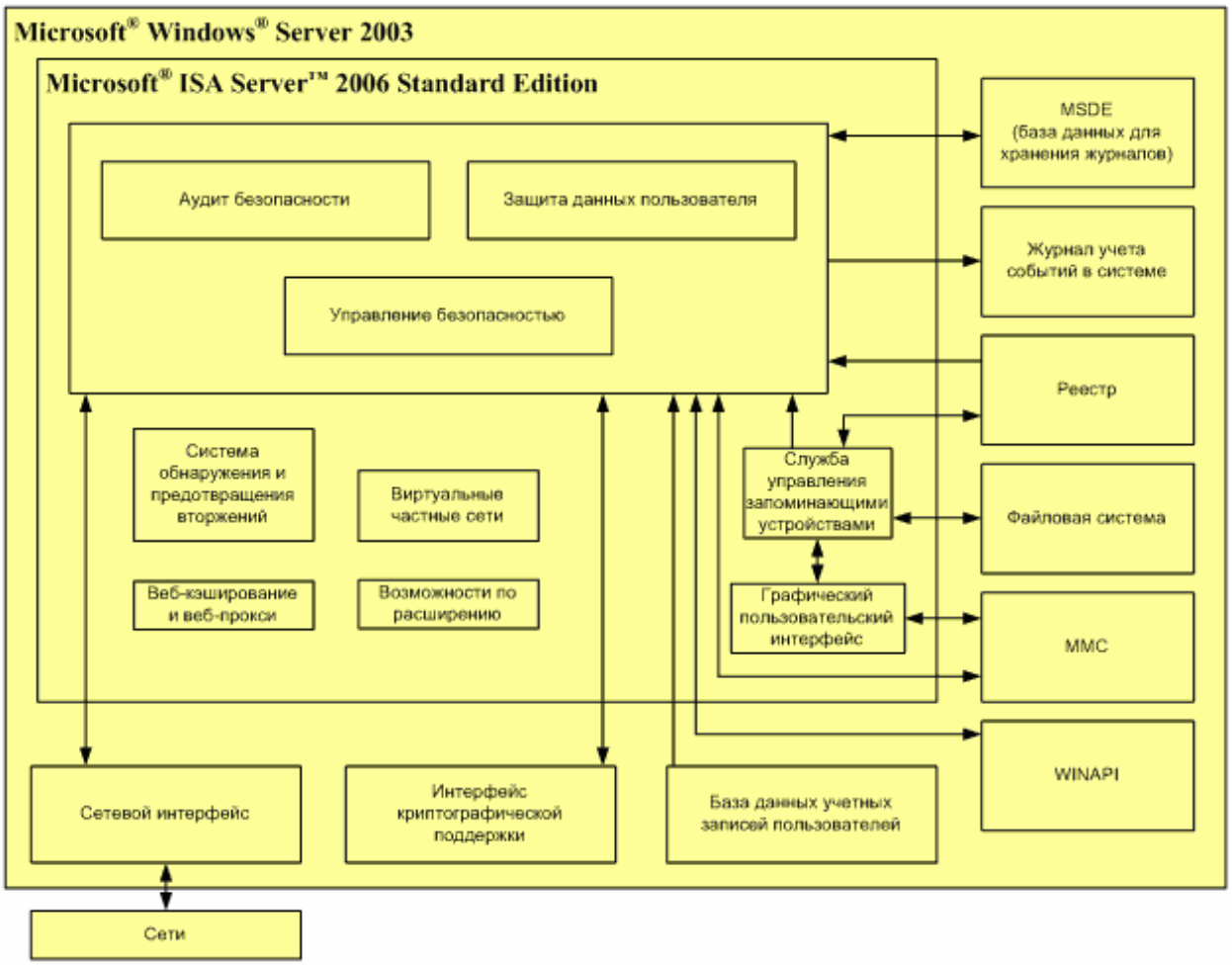

Рисунок 2.2 – Логические границы ОО

В ОО не входят используемые компоненты операционной системы Microsoft® Windows® Server 2003, под управлением которой он функционирует.

Для хранения данных аудита объект оценки использует базу данных MSDE. Данные аудита защищены файловой системой от несанкционированного доступа. Из реестра и файловой системы чтение конфигурационных данных выполняется с использованием службы управления запоминающими устройствами (Storage Service). База данных учетных записей пользователей предоставляет информацию, используемую при идентификации и аутентификации. Интерфейс криптографической поддержки обеспечивает функциональность защищенных протоколов. Сетевой интерфейс необходим для передачи данных в различные сети. MMC требуется одному из компонентов функции безопасности «Аудит безопасности» для отображения данных журнала аудита. WinAPI обеспечивает низкоуровневые функции, используемые ОО.

2.3.3 Физические границы ОО

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

- процессор семейства Intel Pentium III 733 МГц (или более производительный);
- объем оперативной памяти – 512 Мбайт;
- свободное место раздела локального жесткого диска, отформатированного с файловой системой NTFS – 150 Мбайт;
- совместимая с операционной системой сетевая плата для каждой сети, подключенной к компьютеру;
- видеоадаптер и монитор для работы в режиме SVGA 800x600;
- привод CD-ROM или привод DVD;
- клавиатура;
- манипулятор типа «мышь».

2.4 Службы безопасности ОО

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

2.4.1 Аудит безопасности

Объект оценки обеспечивает регистрацию в журнале аудита записей, описывающих события блокирования или передачи сетевых пакетов через ОО, а также предоставляет средства для просмотра, фильтрации и экспорта в текстовый файл этих записей. В журнале аудита фиксируются результаты работы служб веб-прокси и межсетевого экрана. Для обеспечения регистрации записей должны быть сконфигурированы правила доступа, в соответствии с которыми должны обрабатываться пакеты.

Записи аудита содержат информацию об IP-адресе клиента и IP-адресе назначения, выполненном действии (блокирование или передача сетевого пакета), используемом протоколе, пользователе, который был инициатором передачи сетевых пакетов, а также дату, время записи и другие данные.

Журналы аудита могут быть сохранены в базе данных MSDE (используется по умолчанию), в базе данных SQL или в файле (формата W3C или формата ISA Server). В

ОО включена возможность сохранения журнал аудита в базе данных MSDE. Возможности сохранения журнала аудита в базе данных SQL и в файле не входят в ОО.

Объект оценки обеспечивает доступ к журналу аудита только уполномоченным на это администраторам ОО: аудитору ISA Server, аудитору наблюдения ISA Server и полному администратору ISA Server.

Объем одного журнала аудита ограничен 2 Гб, но средство просмотра позволяет отображать информацию из нескольких журналов как поступающую из одного файла. По умолчанию установлено ограничение на общий размер файлов журнала аудита – 8 Гб.

На ОО можно настроить действия при достижении максимального размера журнала аудита – удалить старые файлы с целью высвобождения места для вновь создаваемых журналов или запретить создание новых журналов. Помимо этого предусмотрена возможность выбора автоматического удаления файлов, которые были созданы заданное число дней назад.

Для обобщения или детализации информации журналов межсетевого экрана и веб-прокси в ОО предусмотрена возможность создания отчетов.

С помощью монитора производительности ISA Server можно создавать журналы счетчика, журналы трассировок и предупреждения для наблюдения за показателями производительности ОО.

Объект оценки обеспечивает обнаружение и предотвращение наиболее распространенных форм сетевых вторжений.

2.4.2 Защита данных пользователя

Объект оценки обеспечивает механизм управления информационными потоками, реализуемый в виде правил политики безопасности, применяемых ко всем сетевым соединениям через ОО при входящем (из внешней сети во внутреннюю сеть) или исходящем (из внутренней сети во внешнюю сеть) трафике.

Компьютеры, имеющие доступ к внешним сетям через ОО, относятся к одной или нескольким категориям в зависимости от типа клиента: клиент SecureNAT (не входит в ОО), клиент межсетевого экрана или клиент веб-прокси.

Объект оценки обеспечивает управление информационными потоками на уровне сетевых пакетов и на уровне прикладных протоколов. Управление информационными потоками между сетями осуществляется с использованием:

- сетевых правил;

- правил политики межсетевого экранирования (правил системной политики, правил публикации (веб-серверов и прикладных серверов) и правил доступа);
- специализированных фильтров (веб-фильтров и фильтров приложений).

Объект оценки обеспечивает режим блокировки ОО для защиты ФБО и ресурсов подключенных к нему сетей. Режим блокировки ОО используется в том случае, если в результате атаки были отключены службы межсетевого экранирования.

Объект оценки обеспечивает наличие процедур, предоставляющих возможность возврата ОО к безопасному состоянию после сбоя или прерывания обслуживания.

Объект оценки обеспечивает поддержку установления защищенных соединений (с обеспечением конфиденциальности) с внешними доверенными системами.

2.4.3 Управление безопасностью

Объект оценки позволяет настроить три уровня контроля программного обеспечения ОО в зависимости от роли, назначенной администратору ОО. На ОО предусмотрены следующие административные роли:

- аудитор ISA Server – пользователи и группы, которым назначена эта роль, могут выполнять мониторинг работы ОО и сети, но не могут настраивать функции мониторинга;
- аудитор наблюдения ISA Server – пользователи и группы, которым назначена эта роль, могут выполнять все типы мониторинга, включая конфигурирование журналов, оповещений и других функций, разрешенных для этой роли;
- полный администратор ISA Server – пользователи и группы, которым назначена эта роль, могут выполнять любые настройки на ОО, включая конфигурирование правил, применение сетевых шаблонов и мониторинг.

Администраторы ОО, которым назначены эти роли, могут быть созданы в локальном диспетчере учетных записей безопасности SAM операционной системы Microsoft Windows Server 2003, под управлением которой функционирует ОО, или это могут быть пользователи домена, если ОО является членом домена Active Directory внутренней сети.

Делегирование прав контроля программного обеспечения ОО позволяет предоставлять пользователям, не имеющим административной роли на ОО, делегировать (передавать) определенные административные функции.

Графические панели задач и мастера конфигурации упрощают навигацию и настройку стандартных задач. С помощью мастеров политик межсетевого экрана задаются доступные веб-сайты и контент, а также разрешения на установку подключений между определенными IP-адресами с помощью заданных протоколов и портов для конкретных пользователей или групп пользователей.

Конфигурацию межсетевого экрана можно целиком скопировать в файл XML и передать администратору другого межсетевого экрана, чтобы обеспечить стандартную конфигурацию в рамках всей организации.

Управлять работой ОО можно в удаленном режиме с помощью следующих не входящих в ОО средств:

- оснастки MMC;
- служб терминалов Windows 2000;
- удаленного рабочего стола Windows Server 2003.

Кроме того, удаленное управление службами ОО возможно с помощью сценариев, запускаемых из командной строки.

Возможно создавать оповещения на основе событий и использовать их для запуска и остановки служб межсетевого экрана, а также автоматического выполнения действий на основании заданных критериев.

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 противостоит ОО;
- угроз безопасности, которым должна противостоять среда 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 компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

A.TOEConfig

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

3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

A.LocateTOE

Должна быть исключена возможность несанкционированного физического доступа к компьютеру с установленным ОО.

Предположения, имеющие отношения к персоналу

A.QualifyAdm

Персонал, ответственный за администрирование ОО, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

3.2 Угрозы

3.2.1 Угрозы, которым противостоит ОО

В настоящем ЗБ определены следующие угрозы, которым противостоит ОО.

T.UnauthAccess

1. Аннотация угрозы – осуществление доступа к информации и ресурсам, размещаемым во внутренней (защищаемой ОО) сети, неуполномоченными на это субъектами из внешних сетей.

2. Источники угрозы – субъекты внешних х сетей.

3. Способ реализации угрозы – осуществление доступа к информации и ресурсам, размещаемым во внутренней (защищаемой ОО) сети, с использованием инструментальных средств, поддерживающих возможность межсетевого взаимодействия на сетевом и транспортном уровнях, а также предоставляющих возможность генерации запросов к прикладным сервисам.

4. Используемые уязвимости – недостатки механизмов управления информационными потоками ОО, связанные с возможностью предоставления доступа к информации и ресурсам, размещаемым во внутренней (защищаемой ОО) сети, неуполномоченным на это субъектами из внешних сетей.

5. Вид активов, потенциально подверженных угрозе – информация и ресурсы, размещаемые во внутренней (защищаемой ОО) сети.

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

7. Возможные последствия реализации угрозы – возможность несанкционированного воздействия и использования информации и ресурсов, размещаемых во внутренней (защищаемой ОО) сети.

T.AuditOverflow

1. Аннотация угрозы – осуществление действий злоумышленниками из внутренней (защищаемой ОО) сети и/или внешних сетей, направленных на переполнение объема дискового пространства, выделенного для целей хранения данных аудита.

2. Источники угрозы – злоумышленники из внутренней (защищаемой ОО) и внешних сетей.

3. Способ реализации угрозы – многократное осуществление действий, сопровождаемых генерацией записей аудита в ОО, злоумышленниками из внутренней (защищаемой ОО) сети и/или внешних сетей.

4. Используемые уязвимости – недостатки механизмов генерации данных аудита, связанные с возможностью переполнения объема дискового пространства, выделенного для целей хранения данных аудита.

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

6. Нарушаемые свойства безопасности активов – доступность.

7. Возможные последствия реализации угрозы – потеря данных аудита; невозможность регистрации ОО событий, связанных с безопасностью; осуществление нерегистрируемых злонамеренных действий.

T.MaliciousFailure

1. Аннотация угрозы – осуществление действий злоумышленниками из внутренней (защищаемой ОО) сети и/или внешних сетей, направленных на инициирование сбоев и отказов ОО.

2. Источники угрозы – злоумышленники из внутренней (защищаемой ОО) и внешних сетей.

3. Способ реализации угрозы – осуществление действий с использованием специализированных инструментальных средств, направленных на инициирование сбоев и отказов ОО, злоумышленниками из внутренней (защищаемой ОО) сети и/или внешних сетей.

4. Используемые уязвимости – недостатки механизмов защиты ОО от сбоев и отказов.

5. Вид активов, потенциально подверженных угрозе – программное обеспечение ОО.

6. Нарушаемые свойства безопасности активов – доступность, целостность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; снижение уровня безопасности, предоставляемой ОО, вследствие невозможности восстановления свойств ОО после сбоев и отказов.

3.2.2 Угрозы, которым должна противостоять среда ОО

В настоящем ЗБ определены следующие угрозы, которым должна противостоять среда функционирования ОО.

TE.WiretapAuthQuery

1. Аннотация угрозы – осуществление перехвата злоумышленниками из внутренней (защищаемой ОО) сети и/или внешних сетей аутентификационной информации при аутентификации входящих и исходящих запросов и использование перехваченной информации в целях получения несанкционированного доступа к сервисам внутренней (защищаемой ОО) сети.

2. Источники угрозы – злоумышленники из внутренней (защищаемой ОО) и внешних сетей.

3. Способ реализации угрозы – осуществление перехвата аутентификационной информации, с использованием специализированных инструментальных средств и использование ее для получения несанкционированного доступа к защищаемым сервисам.

4. Используемые уязвимости – недостатки механизмов защиты аутентификационной информации, связанные с возможностью ее перехвата и несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – аутентификационная информация для аутентификации входящих и исходящих запросов.

6. Нарушаемые свойства безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – осуществление несанкционированного доступа к защищаемым ОО сервисам сети.

TE.WiretapAuthAdm

1. Аннотация угрозы – осуществление перехвата злоумышленниками из внутренней (защищаемой ОО) сети и/или внешних сетей аутентификационной информации при удаленной аутентификации администратора ОО и использование перехваченной информации в целях получения несанкционированного доступа к управлению функциональными возможностями ОО.

2. Источники угрозы – злоумышленники из внутренней (защищаемой ОО) и внешних сетей.

3. Способ реализации угрозы – осуществление перехвата аутентификационной информации, с использованием специализированных инструментальных средств и использование ее для получения несанкционированного доступа к ОО.

4. Используемые уязвимости – недостатки механизмов защиты аутентификационной информации, связанные с возможностью ее перехвата и несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – аутентификационная информация для аутентификации администратора ОО.

6. Нарушаемые свойства безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – осуществление несанкционированного доступа к ОО и управлению функциональными возможностями ОО.

TE.MaliciousIntegrity

1. Аннотация угрозы – осуществление модификации злоумышленниками из внутренней (защищаемой ОО) сети и/или внешних сетей программной и информационной части ОО в целях нарушения режимов функционирования ОО и снижение уровня безопасности, предоставляемого ОО.

2. Источники угрозы – злоумышленники из внутренней (защищаемой ОО) и внешних сетей.

3. Способ реализации угрозы – осуществление модификации программной и информационной части ОО, с использованием специализированных инструментальных средств.

4. Используемые уязвимости – недостатки механизмов защиты программной и информационной части ОО, связанные с возможностью их несанкционированной модификации.

5. Вид активов, потенциально подверженных угрозе – программное обеспечение ОО; конфигурационные данные ОО; данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; снижение уровня безопасности, предоставляемого ОО.

3.3 Политики безопасности организации

Объект оценки и среда его функционирования должны следовать следующим правилам политики безопасности организации.

P.NetFiltration

Должна осуществляться фильтрация на сетевом уровне на основе сетевых адресов отправителя и получателя, а также с учетом даты и времени. Должны осуществляться возможности по фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств, по фильтрации с учетом входного и выходного сетевого интерфейса, а также по фильтрации с учетом любых значимых полей сетевых пакетов.

P.TrsptFiltration

Должна осуществляться фильтрация на транспортном уровне запросов на установление виртуальных соединений на основе транспортных адресов отправителя и получателя, а также с учетом даты и времени.

P.ApplFiltration

Должна осуществляться фильтрация на прикладном уровне запросов к прикладным сервисам на основе прикладных адресов отправителя и получателя, а также с учетом даты и времени.

P.RegisterFiltration

Должна обеспечиваться возможность регистрации и учета фильтруемых пакетов, а также запросов на установление виртуальных соединений. В параметры регистрации должны включаться адрес, время и результат фильтрации.

P.LocalAlarm

Должна обеспечиваться возможность локальной сигнализации попыток нарушения правил фильтрации.

P.RegisterAdmEnter

Должна обеспечиваться регистрация входа (выхода) администратора ОО в систему (из системы) либо загрузки и инициализации системы и ее программного останова, при

этом в параметрах регистрации должны указываться дата, время и код регистрируемого события, результат попытки осуществления регистрируемого события, идентификатор администратора ОО, предъявленный при попытке осуществления регистрируемого события.

P.RegisterStartPrg

Должна обеспечиваться возможность регистрации запуска программ и процессов (заданий, задач).

P.AuditFinder

Должно обеспечиваться наличие средств сортировки и поиска событий аудита на основе заданных атрибутов.

P.AccessAdm

Должна обеспечиваться идентификация и аутентификация администратора ОО при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия. При этом должно осуществляться препятствование доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

P.RegisterAdmAction

Должна обеспечиваться регистрация действий администратора ОО по изменению правил фильтрации.

P.Environment

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

P.GenerateTime

Должна быть обеспечена привязка по времени событий, подвергаемых аудиту.

P.ProtectFileSystem

Должна быть обеспечена защита программного обеспечения и конфигурационных фалов ОО на уровне файлов файловой системы ОС от несанкционированного доступа.

P.Manage

Должны быть в наличии надлежащие корректно функционирующие средства администрирования ОО, доступные только уполномоченным администраторам ОО.

P.SecurConnect

Должна обеспечиваться поддержка установления защищенных соединений (с обеспечением целостности и конфиденциальности передаваемой информации) с внешними доверенными системами.

P.IntruderDetect

Должна обеспечиваться возможность обнаружения наиболее распространенных форм сетевых вторжений при взаимодействии внутренней (защищаемой ОО) сети с внешними сетями.

4 Цели безопасности

4.1 Цели безопасности для ОО

O.NetFiltration

Фильтрация на сетевом уровне

ОО должен осуществлять фильтрацию на сетевом уровне на основе сетевых адресов отправителя и получателя, а также с учетом даты и времени. Должны осуществляться возможности по фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств, по фильтрации с учетом входного и выходного сетевого интерфейса, а также по фильтрации с учетом любых значимых полей сетевых пакетов.

O.TrsptFiltration

Фильтрация на транспортном уровне

ОО должен осуществлять фильтрацию на транспортном уровне запросов на установление виртуальных соединений на основе транспортных адресов отправителя и получателя, а также с учетом даты и времени.

O.ApplFiltration

Фильтрация на прикладном уровне

ОО должен осуществлять фильтрацию на прикладном уровне запросов к прикладным сервисам на основе прикладных адресов отправителя и получателя, а также с учетом даты и времени.

O.RegisterFiltration

Регистрация фильтрации

ОО должен обеспечивать возможность регистрации и учета фильтруемых пакетов, а также запросов на установление виртуальных соединений. В параметры регистрации должны включаться адрес, время и результат фильтрации.

O.LocalAlarm

Сигнализация нарушений

ОО должен обеспечивать возможность локальной сигнализации попыток нарушения правил фильтрации.

O.RegisterAdmEnter

Регистрация доступа администратора ОО

ОО должен обеспечивать регистрацию входа (выхода) администратора ОО в систему (из системы) либо загрузки и инициализации системы и ее программного останова, при этом в параметрах регистрации должны указываться дата, время и код регистрируемого события, результат попытки осуществления регистрируемого события, идентификатор администратора ОО, предъявленный при попытке осуществления регистрируемого события.

O.RegisterStartPrg

Регистрация запуска программ и процессов

ОО должен обеспечивать возможность регистрации запуска программ и процессов (заданий, задач).

O.RegisterFeatures

Особенности регистрации

ОО должен обеспечивать наличие средств сортировки и поиска событий аудита на основе заданных атрибутов. ОО должен обеспечивать невозможность потери записей аудита вследствие недостаточности выделенного объема дискового пространства.

O.DisasterRecovery

Безопасное восстановление

ОО должен обеспечивать возможность восстановления после сбоев и отказов оборудования, предусматривающую восстановление свойств ОО.

O.AdminManage

Наличие средств администрирования

ОО должен располагать надлежащими корректно функционирующими средствами администрирования, доступными только уполномоченным администраторам ОО.

O.SecurConnect

Поддержка установления защищенных соединений

ОО должен обеспечивать поддержку установления защищенных соединений (с обеспечением целостности и конфиденциальности передаваемой информации) с внешними доверенными системами.

O.IntruderDetect

Обнаружение вторжений

ОО должен обеспечивать возможность обнаружения наиболее распространенных форм сетевых вторжений при взаимодействии внутренней (защищаемой ОО) сети с внешними сетями.

4.2 Цели безопасности для среды

OE.NonWiretapAuth

Аутентификация запросов

Должна обеспечиваться возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

Примечание

Данная цель безопасности может быть достигнута применением механизмов одноразовой аутентификации, также возможно применение других механизмов безопасности.

OE.AccessAdm

Идентификация и аутентификация администратора ОО

Должна обеспечиваться идентификация и аутентификация администратора ОО при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия. При этом должно осуществляться препятствование доступу

неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

OE.RemovedQuery

Удаленный доступ

При удаленных запросах администратора ОО на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

Примечание

Данная цель безопасности может быть достигнута применением механизмов одноразовой аутентификации, также возможно применение других механизмов безопасности.

OE.RegisterAdmAction

Регистрации действий администратора ОО

Должна обеспечиваться регистрация действий администратора ОО по изменению правил фильтрации.

OE.ControlIntegrity

Обеспечение контроля целостности

Должны быть предусмотрены средства, обеспечивающие контроль целостности программной и информационной части ОО по контрольным суммам.

OE.ImpossibleModif

Стерильность среды функционирования

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

OE.TOEConfig

Надлежащая эксплуатация ОО

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

OE.LocateTOE

Физическая защита ОО

Должна быть исключена возможность несанкционированного физического доступа к компьютеру с установленным ОО.

OE.QualifyAdm

Требования к администраторам ОО

Персонал, ответственный за администрирование ОО, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

OE.Environment

Стойкость функции безопасности

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.GenerateTime

Поддержка аудита

Должна быть обеспечена поддержка средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

OE.ProtectFileSystem

Защита на уровне файловой системы

Должна быть обеспечена защита программного обеспечения и конфигурационных фалов ОО на уровне файлов файловой системы ОС от несанкционированного доступа.

5 Требования безопасности ИТ

В данном разделе ЗБ представлены требования безопасности ИТ, которым должен удовлетворять ОО и его среда. Функциональные требования, представленные в настоящем ЗБ, основаны на функциональных компонентах из части 2 ОК. Требования доверия основаны на компонентах требований доверия из части 3 ОК и представлены в настоящем ЗБ в виде оценочного уровня доверия ОУД1, усиленного компонентом доверия AVA_SOF.1 (Оценка стойкости функции безопасности ОО).

5.1 Требования безопасности для ОО

5.1.1 Функциональные требования безопасности ОО

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

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_ARP.1	Сигналы нарушения безопасности
FAU_GEN.1	Генерация данных аудита безопасности
FAU_SAA.1	Анализ потенциального нарушения
FAU_SAR.1	Просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_STG.4	Предотвращение потери данных аудита
FDP_IFC.1	Ограниченное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_SMR.1	Роли безопасности
FPT_RCV.1	Ручное восстановление
FTP_ITC.1	Доверенный канал передачи между ФБО

5.1.1.1 Аудит безопасности (FAU)

FAU_ARP.1 Сигналы нарушения безопасности

FAU_ARP.1.1 ФБО должны предпринять [действия по локальной сигнализации попыток нарушения правил фильтрации, а также действия по сигнализации обнаружения сетевых вторжений] при обнаружении возможного нарушения безопасности.

Зависимости: FAU_SAA.1 «Анализ потенциального нарушения».

FAU_GEN.1 (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) фильтрация пакетов;

в) запросы на установление виртуальных соединений;

г) вход (выход) администратора ОО в систему (из системы);

д) загрузка и инициализация системы;

е) программный останов системы;

ж) запуск программ и процессов (заданий, задач)

].

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

а) дата и время события, тип **(код)** 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 [адрес отправителя и получателя].

Зависимости: FPT_STM.1 «Надежные метки времени».

FAU_SAA.1 Анализ потенциального нарушения

FAU_SAA.1.1 ФБО должны быть способны применить набор правил мониторинга событий, подвергающихся аудиту, **а также мониторинга**

информационного потока, передающегося через ОО, и указать на возможное нарушение ПБО, основываясь на этих правилах.

FAU_SAA.1.2 ФБО должны реализовать следующие правила при мониторинге событий, подвергающихся аудиту, **а также мониторинге информационного потока, передающегося через ОО**:

а) накопление или объединение известных [событий, связанных с фильтрацией информации], указывающих на возможное нарушение безопасности;

б) [сопоставление перемещаемого информационного потока с известными и наиболее распространенными формами сетевых вторжений].

Зависимости: FAU_GEN.1 (1) «Генерация данных аудита».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [администратору ОО] возможность читать [все данные журнала аудита] из записей аудита.

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

Зависимости: FAU_GEN.1 (1) «Генерация данных аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны предоставить возможность выполнить *фильтрацию, поиск и сортировку* данных аудита, основанные на

[

следующих критериях:

а) времени;

б) адресе отправителя;

в) адресе получателя;

г) номере порта;

д) действии

].

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны выполнить *запись поверх самых старых хранимых записей аудита* и [другие действия по умолчанию не предусмотрены] при **отсутствии свободного дискового пространства для создания журнала аудита**.

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

5.1.1.2 Защита данных пользователя (FDP)

FDP_IFC.1 Ограниченное управление информационными потоками

FDP_IFC.1.1 ФБО должны осуществлять [политику управления информационными потоками] для

[

а) субъектов – сущностей ИТ внешних и внутренней (защищаемой ОО) сетей;

б) информации – сетевого трафика, передающегося через ОО между субъектами;

в) операций – запросов к сервисам, перемещения информации (в том числе пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств)

].

Зависимости: FDP_IFF.1 «Простые атрибуты безопасности».

FDP_IFF.1 Простые атрибуты безопасности

FDP_IFF.1.1 ФБО должны осуществлять [политику управления информационными потоками], основанную на следующих типах атрибутов безопасности **перемещаемой** информации:

[

а) транспортных адресах отправителя и получателя;

б) сетевых адресах отправителя и получателя;

в) входном и выходном интерфейсах;

г) любых значимых полей сетевых пакетов;

д) прикладных адресах отправителя и получателя;

е) дате и времени

].

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

[

а) субъекты внутренней (защищаемой ОО) сети могут передавать информацию или запросы к сервисам через ОО в другую подключенную сеть, если выполняются все следующие условия:
   - значения транспортных и сетевых адресов отправителя и получателя, входных и выходных интерфейсов, любых значимых полей сетевых пакетов являются разрешающими, а также установлены администратором ОО правила обработки сетевых пакетов (трансляция или маршрутизация);
   - администратором ОО заданы правила политики межсетевого экранирования, и все значения прикладных адресов отправителя и получателя являются разрешающими;
   - все значения даты и времени являются разрешающими либо не заданы;

б) субъекты внешней сети могут передавать информацию или запросы к сервисам через ОО во внутреннюю (защищаемую ОО) сеть, если выполняются все следующие условия:
   - значения транспортных и сетевых адресов отправителя и получателя, входных и выходных интерфейсов, любых значимых полей сетевых пакетов являются разрешающими, а также установлены администратором ОО правила обработки сетевых пакетов (трансляция или маршрутизация);
   - администратором ОО заданы правила политики межсетевого экранирования, и все значения прикладных адресов отправителя и получателя являются разрешающими;
   - все значения даты и времени являются разрешающими либо не заданы;

].

FDP_IFF.1.3 ФБО должны [разрешать исходящие и входящие HTTP-запросы, если механизмами среды функционирования ОО проведена их успешная аутентификация или аутентификация не требуется].

FDP_IFF.1.4 ФБО должны предоставить [возможность генерации запросов на аутентификацию исходящих и входящих HTTP-запросов].

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:

[

а) ОО должен отклонять запросы на доступ или запросы к сервисам, в случае, если для отправителя и получателя администратором ОО не установлены правила обработки сетевых пакетов (трансляция или маршрутизация);

б) ОО должен отклонять запросы на доступ или запросы к сервисам, в случае, если для отправителя и получателя администратором ОО не установлены правила политики межсетевого экранирования

].

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

5.1.1.3 Управление безопасностью (FMT)

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления информационными потоками], **предоставляющую** возможность [добавления правила, удаления правила, модификации атрибутов в правиле] атрибутов безопасности [перечисленных в элементе FDP_IFF.1.1 компонента FDP_IFF.1] только [уполномоченному администратору ОО].

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

FMT_MSA.3 Инициализация статических атрибутов

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

FMT_MSA.3.2 ФБО должны предоставить возможность [уполномоченному администратору ОО] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

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

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать **роль** [администратора ОО].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать пользователей с **ролью**.

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

5.1.1.4 Защита ФБО (FPT)

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».

5.1.1.5 Доверенный маршрут/канал (FTP)

FTP_ITC.1 Доверенный канал передачи между ФБО

FTP_ITC.1.1 ФБО должны предоставлять канал связи между собой и удаленным доверенным продуктом ИТ, который логически отличим от других каналов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту данных канала от модификации или раскрытия.

FTP_ITC.1.2 ФБО должны позволить *ФБО и удаленному доверенному продукту ИТ* инициировать связь через доверенный канал.

FTP_ITC.1.3 ФБО должны инициировать связь через доверенный канал **в случае необходимости** [установления защищенных соединений].

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 5.2).

Таблица 5.2 – 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 среды ИТ

Функцией безопасности, реализуемой средой ИТ (операционной системой) в интересах обеспечения безопасности ОО, является функция безопасности «Аутентификация». Данная функция реализуется механизмом паролей среды ИТ (операционной системы). Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости. В качестве минимального уровня стойкости функции безопасности «Аутентификация» в настоящем ЗБ заявлена «**Средняя СФБ**»

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

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.3.

Таблица 5.3 – Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_STG.1	Защищенное хранение журнала аудита
FIA_AFL.1	Обработка отказов аутентификации
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.8 (EXT)	Аутентификация запросов
FIA_UAU.9 (EXT)	Аутентификация при удаленном доступе
FIA_UID.2	Идентификация до любых действий пользователя
FPT_AMT.1	Тестирование абстрактной машины
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени
FPT_TST.1	Тестирование ФБО

5.2.1 Аудит безопасности (FAU)

FAU_GEN.1 (2) Генерация данных аудита

FAU_GEN.1.1 **Функции безопасности среды ИТ** должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

а) запуск и завершение выполнения функций аудита;

б) [действия администратора ОО по изменению правил фильтрации].

FAU_GEN.1.2 **Функции безопасности среды ИТ** 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, [другая, относящаяся к аудиту информация, не определена].

Зависимости: FPT_STM.1 «Надежные метки времени».

FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.1.1 **Функции безопасности среды ИТ** должны защищать хранимые записи аудита от несанкционированного удаления.

FAU_STG.1.2 **Функции безопасности среды ИТ** должны быть способны к *предотвращению* модификации записей аудита.

Зависимости: FAU_GEN.1 (1) «Генерация данных аудита»,
FAU_GEN.1 (2) «Генерация данных аудита».

5.2.2 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 **Функции безопасности среды ИТ** должны обнаруживать, когда произойдет [установленное администратором ОС число (не более 10)] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации администратора ОО].

FIA_AFL.1.2 При **достижении** определенного **в элементе FIA_AFL.1.1** числа неуспешных попыток аутентификации **функции безопасности среды ИТ** 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.2 «Аутентификация до любых действий пользователя».

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 **Функции безопасности среды ИТ** должны предоставить механизм для верификации того, что **пароли на доступ к ОО** отвечают **следующей метрики качества**

[

а) минимальная длина – 6 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 **Функции безопасности среды ИТ** должны требовать, чтобы **администратор ОО при его локальных запросах на доступ** был успешно аутентифицирован **по паролю условно-постоянного действия** до разрешения любого действия, выполняемого при посредничестве ФБО от имени **администратора ОО**.

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

FIA_UAU.8 (EXT) Аутентификация запросов

FIA_UAU.8 (EXT) Функции безопасности среды ИТ должны обеспечивать возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

Зависимости: отсутствует.

FIA_UAU.9 (EXT) Аутентификация при удаленном доступе

FIA_UAU.9 (EXT) Функции безопасности среды ИТ должны обеспечивать идентификацию и аутентификацию методами, устойчивыми к пассивному и активному перехвату информации при удаленных запросах администратора ОО на доступ.

Зависимости: отсутствует.

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 **Функции безопасности среды ИТ** должны требовать, чтобы каждый **администратор ОО при его локальных запросах на доступ** был успешно идентифицирован **по идентификатору (коду)** до разрешения любого действия, выполняемого при посредничестве ФБО от имени **администратора ОО**.

Зависимости: отсутствуют.

5.2.3 Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 **Функции безопасности среды ИТ** должны выполнять пакет тестовых программ *по запросу уполномоченного* ***администратора ОО*** для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая **является базовой для** ФБО.

Зависимости: отсутствуют.

FPT_SEP.1 Отделение домена ФБО

FPT_SEP.1.1 **Функции безопасности среды ИТ** должны поддерживать домен безопасности для выполнения **ФБО**, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 **Функции безопасности среды ИТ** должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 **Функции безопасности среды ИТ** должны быть способны предоставить надежные метки времени для **использования ФБО**.

Зависимости: отсутствуют.

FPT_TST.1 Тестирование ФБО

FPT_TST.1.1 **Функции безопасности среды ИТ** должны выполнять пакет программ **тестирования ФБО** *периодически в процессе нормального функционирования* для демонстрации правильного выполнения ФБО.

FPT_TST.1.2 **Функции безопасности среды ИТ** должны предоставить уполномоченному **администратору ОО** возможность верифицировать целостность данных ФБО **по контрольным суммам**.

FPT_TST.1.3 **Функции безопасности среды ИТ** должны предоставить уполномоченному **администратору ОО** возможность верифицировать целостность хранимого выполняемого кода ФБО **по контрольным суммам**.

Зависимости: FPT_AMT.1 «Тестирование абстрактной машины».

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;
- управление безопасностью.

6.1.1 Функции безопасности «Аудит безопасности»

Функции безопасности ОО «Аудит безопасности» обеспечивают:

- сбор данных аудита;
- сохранение данных аудита;
- просмотр данных аудита;
- защиту журнала аудита от переполнения;
- ограничение доступа к журналу аудита;
- создание отчетов;
- монитор производительности.

6.1.1.1 Сбор данных аудита

Для обеспечения регистрации в журнале аудита записей, описывающих события блокирования или передачи сетевых пакетов через ОО, должны быть сконфигурированы соответствующие правила доступа, в соответствии с которыми данные пакеты обрабатывались.

В журнале аудита фиксируются следующие службы:

- служба веб-прокси;
- служба межсетевого экрана.

Возможно сконфигурировать журнал аудита отдельно для каждой службы. Процедура конфигурирования журнала веб-прокси аналогична процедуре конфигурирования журнала межсетевого экрана. Одно из главных отличий состоит в

доступных полях. При этом можно настраивать поля, которые будут фиксироваться в журналах аудита.

Журнал регистрации службы веб-прокси обеспечивает аудит каждого HTTP-запроса, обрабатываемого ОО. При этом происходит регистрация всех запросов, как входящих, так и исходящих.

Журнал регистрации служб межсетевого экранирования содержит записи аудита для сетевых пакетов, которые были отклонены пакетным фильтром ОО. При этом ОО также поддерживает возможность регистрации сетевых пакетов, которые были успешно переданы через ОО.

Если служба межсетевого экрана остановлена вручную или автоматически, средство просмотра журнала аудита прекратит обновление информации, ОО перейдет в режим изоляции. Данное событие требует вмешательства администратора ОО для возврата ОО к нормальному функционированию.

6.1.1.2 Сохранение данных аудита

Журналы аудита могут быть сохранены:

- в базе данных MSDE – используется по умолчанию;
- в базе данных SQL – может использоваться в том случае, если в сети имеется SQL Server;
- в файле (формата W3C или формата ISA Server).

По умолчанию информация журналов аудита сохраняется в базе данных MSDE.

Журнал аудита в MSDE сохраняется в папке ISALogs, находящейся внутри папки, в которую установлен ОО. При необходимости, можно изменить место хранения файлов журналов в MSDE.

Возможности сохранения журналов аудита в БД SQL Server и в файл не входят в оцениваемую конфигурацию и вынесены за рамки ОО.

6.1.1.3 Просмотр данных аудита

Средство просмотра журналов аудита показывает все сделанные записи в реальном масштабе времени. Событие отображается сразу же после его фиксации в журнале. Фильтр по умолчанию отображает все записи для журналов межсетевого экрана и веб-прокси.

По умолчанию будут показаны следующие столбцы при просмотре журнала аудита:

- время записи;
- IP-адрес клиента;
- порт назначения;
- используемый протокол;
- действие;
- правило;
- IP-адрес назначения;
- имя пользователя клиента;
- исходная сеть;
- сеть назначения;
- HTTP-метод;
- URL-адрес.

Можно добавить дополнительные столбцы, например, MIME type, прокси-адресат или прокси-источник, сервер ссылок и многие другие.

Средство просмотра журналов аудита можно также использовать для отображения информации, сохраненной с помощью MSDE. При этом можно создавать запросы к БД и отыскивать нужную информацию с использованием фильтров. Отображаться будут только записи, отвечающие всем заданным критериям. Это одно из основных преимуществ формата MSDE над другими форматами, которые могут быть использованы для хранения журналов аудита.

Для фильтра можно выбрать следующие критерии:

- HTTP-метод;
- IP-адрес клиента;
- IP-адрес назначения;
- MIME-тип;
- URL-адрес;
- агент клиента;
- время записи;
- время записи (GMT);
- время обработки;
- данные кэширования;

- двунаправленный;
- действие;
- заголовок Raw IP;
- имя пользователя клиента;
- имя сервера;
- имя узла клиента;
- имя узла назначения;
- используемый протокол;
- источник объекта;
- исходная сеть;
- исходный IP-адрес клиента;
- исходный прокси;
- код результата;
- код состояния HTTP;
- необработанные полезные данные;
- отправлено байт;
- отсылающий сервер;
- получено байт;
- порт источника;
- порт назначения;
- правило;
- прокси назначения;
- прошедший проверку клиент;
- сведения о фильтре;
- сведения об ошибке;
- сервер проверки подлинности;
- сетевой интерфейс;
- сеть назначения;
- служба;
- тип записи журнала;
- транспорт.

При хранении журнала аудита в БД MSDE можно проводить фильтрование по времени регистрации. Это позволяет отображать данные, заносимые за определенный

период времени. При этом время регистрации можно задать отличным от текущего (offline просмотр).

По умолчанию отображается текущее время регистрации – и это единственное значение, если записи производятся не в БД MSDE. Если же запись ведется в БД MSDE, то можно выбрать следующие варианты:

- последние 24 часа;
- последние 30 дней;
- последние 7 дней;
- последний час;
- непосредственное время;
- не позднее;
- не ранее.

Некоторые из этих критериев применимы только к одному или двум типам журналов аудита (межсетевой экран или веб-прокси).

После конфигурирования типа записи журнала можно выбрать отображаемые записи из фильтра межсетевого экрана или веб-прокси, только из фильтра межсетевого экрана или только из фильтра веб-прокси.

Определения фильтра просмотра журнала аудита можно сохранить в xml-файлах и импортировать их по мере необходимости. Данная возможность полезна в тех случаях, когда имеется очень много различных критериев фильтрования данных журнала аудита. После конфигурирования способа записи журнала, можно выбрать отображение записей от фильтра межсетевого экрана или веб-прокси, только от фильтра межсетевого экрана или только от веб-прокси.

С помощью средства просмотра журнала аудита можно экспортировать информацию в текстовый файл, который удобно анализировать с помощью различных программных средств.

6.1.1.4 Защита журнала аудита от переполнения

Объем одного журнала аудита ограничен 2 Гб, но средство просмотра позволяет отображать информацию из нескольких журналов как поступающую из одного файла. Когда объем журнала аудита достигает 2 Гб, ОО автоматически начинает новый журнал.

По умолчанию установлено ограничение на общий размер файлов журнала аудита – 8 Гб, а размер свободного дискового пространства, необходимого для обслуживания

операций мониторинга – 2 Гб. При этом для файлов формата MSDE не предусмотрена возможность сжатия.

На ОО можно настроить действие при достижении максимального размера журнала аудита:

- удалить старые файлы с целью высвобождения места для вновь создаваемых журналов;
- запретить создание новых журналов.

Также предусмотрена возможность выбора автоматического удаление файлов, которые были созданы заданное число дней назад. По умолчанию выбран именно этот вариант, а период времени по умолчанию равен 7 дням.

6.1.1.5 Ограничение доступа к журналу аудита

Для просмотра содержимого журнала аудита пользователь должен быть определен в одной (или нескольких) из административных ролей, предусмотренных на ОО.

6.1.1.6 Создание отчетов

Создание отчетов используется для обобщения или детализации информации журналов межсетевого экрана и веб-прокси способом, который позволяет анализировать данные и их отдельные фрагменты, тенденции и аномалии, например, отслеживать использование полосы пропускания канала передачи данных для перераспределения потоков или же отслеживать доступ в целях обеспечения безопасности.

Предусмотрена возможность создания отчетов вручную или по расписанию. По умолчанию средство создания отчетов создает базу данных в папке ISA Summaries компьютера, на котором установлен ОО.

При создании отчета вручную нужно выбрать отчетный период (дату начала и конечную дату) и тип содержимого, которое должно быть включено в отчет. Можно выбрать один или несколько из следующих типов содержимого:

- сводка;
- использование Интернета;
- использование приложения;
- трафик и загрузка;
- безопасность.

Также можно настроить отправку уведомления по электронной почте после создания отчета и публикацию отчета в каталог. Публикация необходима в том случае, если отчеты должны просматриваться на других компьютерах. Для этого необходимо установить путь к каталогу или выбрать папку для сохранения отчета. Возможно, потребуется ввести имя учетной записи и пароль для учетной записи, чтобы получить возможность записи в определенный каталог. Отчет автоматически сохраняется в формате HTML. После создания отчета его можно просматривать в веб-браузере. Если при конфигурации задания на отчет не выбран вариант автоматической публикации отчета в каталог, можно опубликовать отчет после его создания вручную.

Создание отчетов на регулярной основе используется для автоматического создания ежедневных, еженедельных, ежемесячных и ежегодных отчетов. Данная опция предоставляет дополнительное удобство при сопоставлении результатов.

Если выбран вариант еженедельного запуска задания на отчет, можно выбрать день недели запуска задания. Если задание должно выполняться ежемесячно, то необходимо будет задать день месяца, в который задание должно выполняться. Если необходим отчет, который охватывает весь предшествующий месяц, то необходимо установить это значение в 1 (первое число месяца).

Как и при создании одноразового отчета, при создании отчета на регулярной основе можно сконфигурировать задание на публикацию отчетов в каталог, а также сообщение электронной почты, которое необходимо отправить по завершении отчета.

Возможно настроить каждый тип содержимого отчета:

- настроить содержимое итогового отчета – определить количество протоколов, определить число пользователей в отчете, задать способ сортировки для определения самых нагруженных сайтов, а также определить порядок сортировки по использованию кэша: по запросам или по байтам;
- настроить содержимое веб-ресурсов – определить число протоколов и определить порядок сортировки для определения важнейших протоколов, определить число важнейших веб-сайтов и порядок сортировки, определить число важнейших пользователей и порядок их сортировки, определить число типов объектов и порядок их сортировки, определить число веб-браузеров и порядок их сортировки, а также определить число операционных систем и порядок их сортировки;

- настроить содержимое ресурсов приложений – определить число важнейших протоколов и порядок их сортировки, число важнейших пользователей и порядок их сортировки, число клиентских приложений и порядок их сортировки, число адресатов и порядок их сортировки, а также число операционных систем и порядок их сортировки;
- настроить содержимое трафика и использования – определить число важнейших протоколов и порядок сортировки по использованию кэша;
- настроить содержимое безопасности – определить число клиентов, которые создают наибольшее число отброшенных пакетов, и число пользователей, которые создают наибольшее число проблем с авторизацией.

6.1.1.7 Монитор производительности

При установке программного обеспечения ОО устанавливается монитор производительности ISA Server (особым образом настроенный системный монитор Windows, в который включены только счетчики производительности, связанные с ОО).

В мониторе производительности ISA Server содержатся счетчики для следующих объектов:

- ISA Server Firewall Packet Engine;
- ISA Server Firewall Service;
- ISA Server Web Proxy.

Для выбранного объекта можно добавлять или удалять счетчики. Можно добавить счетчики для любого объекта, относящиеся не только к ОО.

Монитор производительности ISA Server конфигурируется тем же способом, что и монитор производительности Windows, при этом можно создавать журналы счетчика, журналы трассировок и предупреждения точно так же, как при наблюдении за другими показателями операционной системы Windows.

6.1.1.8 Обнаружение вторжений

Объект оценки располагает механизмами обнаружения и предотвращения наиболее распространенных форм сетевых вторжений. Данные механизмы обеспечивают распознавание попытки атаки определенного типа, уведомление администратора ОО и выполнение заранее заданных действий.

Сопоставление с ФТБ

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

- FAU_ARP.1 – ФБО осуществляют локальную сигнализацию попыток нарушения правил фильтрации, а также действия по сигнализации обнаружения сетевых вторжений;
- FAU_GEN.1 (1) – ФБО обеспечивают генерацию данных аудита для следующих событий: запуск и завершение выполнения функций аудита, фильтрация пакетов, запросы на установление виртуальных соединений, вход (выход) администратора ОО в систему (из системы), загрузка и инициализация системы, программный останов системы, запуск программ и процессов (заданий, задач). Для каждого события аудита ФБО регистрируют дату, время, тип (код) события, идентификатор субъекта, результат события, адрес отправителя и получателя;
- FAU_SAA.1 – ФБО обеспечивают применение набора правил мониторинга событий, подвергающихся аудиту, а также мониторинга информационного потока, передающегося через ОО, и указывают на возможное нарушение ПБО, основываясь на этих правилах, а также осуществляют накопление или объединение событий, связанных с фильтрацией информации, указывающих на возможное нарушение безопасности и сопоставление перемещаемого информационного потока с известными и наиболее распространенными формами сетевых вторжений;
- FAU_SAR.1 – инструментальные средства просмотра событий предоставляют администратору ОО возможность просмотра данных аудита в удобочитаемом формате;
- FAU_SAR.3 – инструментальные средства просмотра событий аудита предоставляют возможность выполнения поиска данных аудита по различным атрибутам;
- FAU_STG.4 – ФБО выполняют запись поверх самых старых хранимых записей аудита при отсутствии свободного дискового пространства для создания журнала аудита.

6.1.2 Функции безопасности «Защита данных пользователя»

Объект оценки обеспечивает механизм управления информационными потоками, реализуемый в виде правил политики безопасности, применяемых ко всем сетевым соединениям через ОО при входящем (из внешней сети во внутреннюю сеть) или исходящем (из внутренней сети во внешнюю сеть) трафике.

Компьютеры, имеющие доступ к внешним сетям через ОО, относятся к одной или нескольким категориям в зависимости от типа клиента:

- клиент SecureNAT (не входит в ОО);
- клиент межсетевого экрана;
- клиент веб-прокси.

Отдельный компьютер может играть роль различных типов клиента ОО.

Объект оценки обеспечивает управление информационными потоками на уровне сетевых пакетов и на уровне прикладных протоколов. При этом контроль осуществляется до того, как информация сможет быть передана через ОО. Управление информационными потоками между сетями осуществляется с использованием:

- сетевых правил;
- правил политики межсетевого экранирования (правил системной политики, правил публикации (веб-серверов и прикладных серверов) и правил доступа);
- специализированных фильтров (веб-фильтров и фильтров приложений).

Правила публикации (веб-сервера и прикладных серверов) и правила доступа составляют политику доступа.

Для облегчения процесса конфигурирования сетевых правил и правил политики межсетевого экранирования для управления трафиком между несколькими сетями в ОО используются сетевые шаблоны, включающие наиболее распространенные схемы сетей.

Стандартную конфигурацию межсетевого экрана после установки можно представить так:

- системные политики разрешают выборочный трафик с/на ОО;
- запрещен весь трафик через ОО, потому что есть только одно запрещающее правило;
- между сетями VPN-клиентов и VPN клиентов, помещенных в карантин, с одной стороны и внутренней сетью установлены отношения типа «маршрут»;
- между внутренней сетью и внешней сетью по умолчанию задано отношение трансляции адресов NAT;

- только администраторы ОО могут менять политику.

Когда ОО получает запрос на соединение, он, выполняет проверки в следующем порядке:

- проверка наличия сетевого правила, определяющего маршрут между сетью-источником информации и сетью-адресатом. Если такого сетевого правила нет, ОО предполагает, что сеть-источник и сеть-адресат не соединены;
- в том случае, если ОО подтвердил маршрут между сетью-источником информации и сетью-адресатом, рассматривается политика доступа. ОО обрабатывает правила в политике доступа сверху вниз (системная политика реализуется до выполнения политики доступа, определенной пользователем);
- если запрос на соединение не соответствует параметрам в правиле, ОО переходит к рассмотрению следующего правила в политике доступа;
- если запрос на соединение соответствует параметрам в правиле, ОО снова проверяет сетевые правила, чтобы выяснить, применяется ли NAT или маршрутизация для связи между сетью-источником и сетью-адресатом, а также наличие правил построения цепочек связывания в веб (если клиент веб-прокси запросил объект) или возможную конфигурацию связывания (если клиент SecureNAT или клиент межсетевого экрана затребовали объект). В зависимости от конфигурации правила, ОО разрешит или запретит выполнение запроса;
- если не задана системная политика или определенные пользователем правила, предназначенные для запроса на соединение, то применяется последнее правило по умолчанию. Это правило блокирует все коммуникации через ОО.

6.1.2.1 Типы клиентов ОО

Клиент межсетевого экрана

Программное обеспечение клиента межсетевого экрана – вспомогательный программный продукт, который можно установить на любую операционную систему, совместимую с Windows, для обеспечения защиты и доступа через ОО. Клиенты межсетевого экрана могут выполнять соединения из сетей периметра и внутренних сетей. Все остальные типы сетей не поддерживаются.

Программное обеспечение клиента межсетевого экрана реализует следующие функции:

- позволяет выполнять строгую пользовательскую/групповую проверку подлинности для всех приложений Winsock, использующих протоколы TCP и UDP;
- позволяет вносить в системные журналы ОО информацию о пользователях и приложениях;
- обеспечивает расширенную поддержку сетевых приложений, включая сложные протоколы, требующие вторичных соединений;
- обеспечивает DNS-поддержку компьютеров клиентов межсетевого экрана;
- позволяет публиковать серверы, требующие использования сложных протоколов без помощи фильтров приложений;
- маршрутная инфраструктура сети прозрачна для клиента межсетевого экрана.

В отличие от клиента SecureNAT клиент межсетевого экрана может получить доступ практически к любому протоколу TCP/UDP, в том числе к сложным протоколам, требующим несколько первичных и/или вторичных соединений без помощи дополнительных фильтров приложений.

Объект оценки может разрешать имена от имени клиентов межсетевого экрана. Это позволяет снять с клиента межсетевого экрана необходимость разрешать имена для хостов во внешней сети и позволяет ОО иметь DNS-кэш недавних запросов на разрешение имен. Функция DNS-поддержки расширяет возможности обеспечения защиты для клиента межсетевого экрана вследствие того, что она исключает необходимость настройки клиента межсетевого экрана на использование общего DNS-сервера для разрешения имен хостов.

Программное обеспечение клиента межсетевого экрана следует устанавливать на опубликованном сервере, для которого необходимо обеспечить поддержку сложных протоколов (например, FTP-сервер).

Для контрольного канала клиента межсетевого экрана использует порт TCP 1745. По этому контрольному каналу клиент межсетевого экрана осуществляет взаимодействие со службой ОО для выполнения разрешения имен и команд сетевых приложений. Служба межсетевого экрана использует информацию, полученную по контрольному каналу, и устанавливает соединение между клиентом межсетевого экрана и сервером-адресатом.

Клиент веб-прокси

В качестве клиента веб-прокси может выступать любой компьютер, браузер которого настроен на использование ОО в качестве сервера веб-прокси. Для настройки компьютера в качестве клиента веб-прокси, отсутствует необходимость в установке дополнительного программного обеспечения. Необходимо только настроить на клиентском компьютере браузер на использование ОО в качестве веб-прокси. Другие приложения также могут быть настроены в качестве клиентов веб-прокси, например, программы обмена сообщениями или клиенты электронной почты.

Программное обеспечение клиента веб-прокси реализует следующие функции:

- улучшает производительность конфигурации клиента межсетевого экрана и клиента SecureNAT для обеспечения веб-доступа;
- позволяет использовать сценарий автоматического конфигурирования для того, чтобы обходить сайты с помощью прямого доступа;
- позволяет обеспечивать веб-доступ (HTTP/HTTPS/FTP), не разрешая пользователям доступ к другим протоколам;
- позволяет осуществлять пользовательский/групповой контроль доступа для веб-доступа;
- поддерживает проверку подлинности RADIUS для исходящих запросов клиента веб-прокси;
- позволяет ограничить количество исходящих соединений клиента веб-прокси;
- поддерживает создание цепочек веб-прокси, которые могут ускорить доступ к внешним сетям.

Компьютеры клиента веб-прокси взаимодействуют с ОО напрямую через фильтр веб-прокси межсетевого экрана. Клиент веб-прокси устанавливает прямое соединение с портом TCP 8080 на ОО. Порт TCP 8080 используется прослушивателем веб-прокси ОО, который прослушивает исходящие веб-запросы, а затем применяет к этим соединениям политики доступа межсетевого экрана. Это повышает производительность, потому что соединения клиентов межсетевого экрана и SecureNAT должны передаваться на фильтр веб-прокси вместо того, чтобы фильтр получал их напрямую. Компьютеры клиента веб-прокси получают доступ к веб-содержимому значительно быстрее.

Одной из значимых функций конфигурации клиента веб-прокси является способность использовать прямой доступ для того, чтобы обходить фильтр веб-прокси для выбранных веб-сайтов.

В том случае, если компьютер клиента веб-прокси настроен на использование сценария автоматического конфигурирования, клиенту веб-прокси предоставляется централизованный список веб-сайтов, к которым можно получить доступ с помощью прямого доступа. Для сайтов, настроенных на прямой доступ, компьютер клиента веб-прокси не будет использовать фильтр веб-прокси, а будет использовать другие методы установки соединения с веб-сайтом, например конфигурацию клиента SecureNAT или межсетевого экрана.

Клиент веб-прокси поддерживает только протоколы HTTP, HTTPS и FTP-загрузки по HTTP-туннелю. Если компьютер пользователя настроен только как клиент веб-прокси, то пользователь этого компьютера имеет доступ только к этим протоколам.

Количество соединений клиента веб-прокси может быть ограничено определенным числом. Данная возможность используется в тех случаях, когда пропускная способность ограничена или нужно сделать так, чтобы лишь определенное количество пользователей получало доступ к внешней сети одновременно.

Клиенты веб-прокси используют туннельное соединение, когда они отправляют свои внешние запросы на ОО. Например, когда пользователь отправляет запрос к сайту, клиент веб-прокси добавляет к этому запросу еще один HTTP-заголовок, в котором в качестве адреса назначения указан внутренний интерфейс компьютера с ОО, а в качестве порта назначения — порт TCP 8080. Когда ОО получает этот запрос, он отбрасывает заголовок клиента веб-прокси и перенаправляет запрос на внешний сайт.

Точно такой же механизм используется в случае, когда клиент веб-прокси отправляет FTP-запрос. Клиент веб-прокси добавляет к FTP-запросу HTTP-заголовок, в котором в качестве адреса назначения указан внутренний интерфейс ОО, а в качестве порта назначения – порт TCP 8080. Когда ОО получает этот запрос, он удаляет HTTP-заголовок и перенаправляет запрос на FTP-сервер в виде FTP-запроса. Поэтому поддержка протокола FTP клиентом веб-прокси обозначается как поддержка FTP по HTTP-туннелю.

6.1.2.2 Сетевые правила

Основной функциональной возможностью ОО является контроль трафика между сетью-источником информации и сетью-адресатом.

В ОО реализована многосетевая модель, которая подходит для соединенных между собой сетей. Для любого соединения между конкретной сетью источника и сетью назначения необходимо задать сетевое правило. Базовый принцип работы с несколькими сетями в ОО – ни одна сеть не является надежной по умолчанию и все соединения, выполняемые через ОО, подвергаются фильтрации с отслеживанием соединений и проверке с отслеживанием соединений на уровне приложения.

Функция поддержки нескольких сетей в ОО облегчает задачу по обеспечению защиты сети от внутренних и внешних угроз безопасности путем ограничения взаимодействия между клиентами даже в пределах одной организации. Функция поддержки нескольких сетей может работать со сложными схемами сети демилитаризованной зоны (также называемой экранированной подсетью), позволяя настраивать способы получения клиентами доступа к сети демилитаризованной зоны в различных сетях.

По завершению установки на ОО создаются следующие сети по умолчанию:

– сеть VPN-клиентов – включает адреса, присвоенные VPN-клиентам;
– сеть VPN-клиентов, помещенных в карантин – включает адреса, присвоенные VPN-клиентам, помещенным в карантин;
– внешняя сеть – включает адреса, которые не принадлежат никакой другой сети;
– внутренняя сеть – включает адреса первичной защищенной сети;
– сеть локального компьютера – включает IP-адреса на ОО.

В дополнение к создаваемым по умолчанию сетям можно конфигурировать пользовательские сети. Новую сеть нельзя использовать до тех пор, пока не будут определены отношения маршрутизации между этой сетью и другими сетями, с которыми она взаимодействует. Эти отношения маршрутизации регулируются с помощью сетевых правил.

Сетевые правила позволят определить следующие типы связи между различными сетями, подключенными к ОО:

– трансляция сетевых адресов – при использовании данного типа подключения сети к объекту оценки, ОО заменяет IP-адрес клиента во внутренней сети источника на собственный внешний IP-адрес для всех исходящих пакетов данных, скрывая, таким образом, используемую во внутренней сети IP-адресацию;

– маршрутизация – при использовании данного типа соединения, клиентские запросы из сети источника напрямую транслируются в сеть назначения. При этом адрес клиента в сети источника включается в запрос.

Маршрут используется, когда сети источника и адресата, определенные в сетевом правиле, поддерживают маршрутизацию между собой. Например, если в сети источника и в сети адресата используются общие адреса или в сети источника, и в сети адресата используются частные адреса, то между ними можно задать отношение типа «маршрут». Если же в сети источника используются частные адреса, а в сети адресата – общие адреса, то этот тип отношения использовать нельзя (в некоторых случаях есть исключения из этого правила).

Маршрутизируемые сети являются двунаправленными, то есть если маршрутизация настроена из одной сети в другую в одном направлении, то она также поддерживается и в обратной направлении. Механизм трансляции сетевых адресов является однонаправленным. Если трансляция сетевых адресов определена из одной сети в другую в одном направлении, то она может быть не определена в обратном направлении.

6.1.2.3 Правила политики межсетевого экранирования

Правила политики межсетевого экранирования представляют собой упорядоченный список, при этом параметры соединения сначала сравниваются с правилом, идущим первым в списке. Перемещение вниз по списку правил выполняется до тех пор, пока не будет найдено правило, соответствующее параметрам соединения. Если такое правило найдено, активируется его политика. Такой подход к политике межсетевого экранирования существенно упрощает локализацию неисправностей и определение причин разрешения или запрещения конкретного соединения. Можно изменить порядок определенных пользователем правил (правил публикации и доступа), но нельзя изменить порядок правил системной политики.

Правила политики межсетевого экранирования реализуются посредством правил:

- системной политики;
- публикации (веб-серверов и прикладных серверов);
- доступа.

По умолчанию правила системной политики позволяют ОО взаимодействовать со службами сетевой инфраструктуры во внутренней сети.

Правила публикации (веб-сервера и прикладных серверов) и правила доступа составляют политику доступа. Политика доступа определяет способ доступа хостов защищенных сетей к хостам других сетей.

Правила публикации веб-сервера и обычного сервера используются для предоставления входящего доступа. Правила публикации следует применять, если необходимо разрешить соединения хоста, не входящего в защищенную ОО сеть, с хостом, размещенным в сети, защищенной ОО.

Правила доступа применяются для управления исходящим доступом от хоста, размещенного в сети, защищенной ОО, с хостом, не входящим в защищенную сеть.

Правила системной политики

Системная политика – это предустановленный набор из 30 правил доступа, позволяющих ОО взаимодействовать со службами сетевой инфраструктуры во внутренней сети. Системная политика ОО является набором правил доступа, которые контролируют входящий и исходящий доступ к/от ОО. Данные правила создаются по умолчанию, но их можно изменить или, при желании, отключить.

К правилам системной политики относятся следующие:

- разрешить доступ к службам каталогов в целях проверки подлинности;
- разрешить проверку подлинности Kerberos с ОО на надежные серверы;
- разрешить установку соединений по протоколу Microsoft CIFS с ОО на надежные серверы;
- разрешить установку соединений по интерфейсу NetBIOS с ОО на надежные серверы.

Для каждого из правил доступа системной политики соединения по умолчанию считаются от сети локального хоста к внутренней сети. Внутренняя сеть для ОО – это сеть, в которой расположены основные серверы сетевой инфраструктуры. Таким образом, правила системной политики по умолчанию разрешают соединения с серверами Active Directory, DNS-, DHCP-, WINS-серверами и файловыми серверами организации. Это представление о внутренней сети применяется для того, чтобы упростить установку ОО, потому что внутренняя сеть определяется в процессе установки программного обеспечения ОО. Определение внутренней сети не накладывает на пользователей никаких ограничений.

В случае прекращения работы служб межсетевого экранирования, ОО переходит в режим блокировки. В данном режиме разрешен только сетевой трафик, определяемый правилами политики режима блокировки. Это сделано с той целью, чтобы предоставить администратору ОО возможность устранять возникшие проблемы с данным компьютером удаленно и не скомпрометировать защищаемые ОО ресурсы сетей.

Правила публикации веб-серверов

Объект оценки использует правила веб-публикации (правила публикации веб-серверов) для обеспечения безопасной публикации HTTP-, HTTPS- и FTP-серверов во внешних сетях.

Правила веб-публикации определяют, каким образом ОО должен обрабатывать входящие HTTP-запросы к ресурсам, расположенным на внутреннем веб-сервере, а также каким образом ОО должен возвращать информацию пользователю, который запросил данные ресурсы.

По существу, правила веб-публикации обеспечивают обработку входящих запросов и их перенаправление на соответствующий веб-сервер, расположенный за ОО во внутренней сети. При этом ОО поддерживает задание правил веб-публикации, предусматривающих и не предусматривающих аутентификацию пользователей при доступе к защищаемым ресурсам.

Правила публикации веб-сервера предоставляют следующие функциональные возможности:

- обеспечение доступа через прокси к веб-сайтам, защищенным ОО;
- контроль прикладного уровня над соединениями, устанавливаемыми с опубликованными веб-сайтами;
- перенаправление маршрута;
- предварительная аутентификация соединений, устанавливаемых с опубликованными веб-сайтами;
- обратное кэширование опубликованных веб-сайтов;
- публикация нескольких веб-сайтов с помощью единственного IP-адреса;
- перезапись URL-адреса, возвращаемого опубликованным веб-сайтом (с помощью преобразования ссылок);
- поддержка передачи на веб-сайт как IP-адреса ОО, так и действительного IP-адреса клиента;

- поддержка системы аутентификации SecurID;
- поддержка системы подтверждения подлинности RADIUS;
- возможность задания расписания, в соответствии с которым разрешаются соединения с опубликованными веб-сайтами;
- переадресация портов и протоколов.

Правила публикации веб-сервера обеспечивают доступ через прокси к веб-сайтам, находящимся в сети, защищенной ОО. Любая сеть, не являющаяся частью внешней сети по умолчанию, рассматривается как сеть, защищенная ОО.

Фильтр веб-прокси ОО обрабатывает все входящие веб-соединения, устанавливаемые с применением правил публикации веб-сервера.

Соединение через прокси более безопасно, чем соединение с определением маршрута или соединение средствами NAT, поскольку соединение разбивается на части и восстанавливается ОО. Оно позволяет ОО выполнять на уровне приложений детальную проверку веб-запросов к веб-сайтам, опубликованным с помощью правил публикации веб-серверов. Проверка на уровне приложений препятствует отправке нарушителем злонамеренных команд или кода на опубликованный веб-сайт.

За контроль на прикладном уровне веб-запросов отвечает HTTP-фильтр ОО. HTTP-фильтр позволяет контролировать практически любой аспект HTTP-соединения и блокировать или разрешать соединения, основанные на компоненте HTTP-коммуникаций.

Правила публикации веб-сервера позволяют публиковать многочисленные веб-сайты, используя один IP-адрес во внешнем интерфейсе ОО. Это возможно благодаря способности ОО выполнять на уровне приложений проверку, отслеживающую соединения. Частью механизма такой проверки служит способность ОО анализировать заголовок хоста во входящем запросе и принимать решение об обработке входящего запроса на основе информации заголовка хоста. Все, что потребуется, – создать соответствующее количество правил публикации веб-серверов. Каждое их них будет ожидать (прослушивать) входящие соединения к указанному сайту и передавать эти запросы на опубликованный с помощью ОО веб-сервер.

Преобразователь ссылок может перезаписывать ответы, которые опубликованные веб-серверы посылают пользователям, сделавшим запрос. Преобразователь ссылок используется при публикации веб-сайтов, включающих в свои ответы жестко закодированные URL-адреса, недоступные с удаленных компьютеров. Преобразователь

ссылок разрешает проблему, перезаписывая ответы, возвращаемые обратившемуся к веб-сайту пользователю.

Объект оценки предоставляет выбор между пересылкой опубликованному веб-серверу IP-адреса ОО и передачей истинного IP-адреса удаленного веб-клиента на опубликованный веб-сервер. Если в журналах регистрации веб-сервера реальный IP-адрес клиента не нужен, можно использовать установку по умолчанию, заменяющую IP-адрес клиента адресом сетевого интерфейса ОО.

Правила публикации веб-сервера, определенные в ОО, дают возможность задавать время доступа пользователей к опубликованному веб-сайту, применяя как встроенные, так и пользовательские расписания в правилах публикации веб-серверов.

С помощью правил публикации веб-сервера можно также выполнять переадресацию портов и протоколов. Переадресация портов дает возможность принять запрос на соединение с одним портом, а затем передать запрос на дублирующий или резервный порт опубликованного веб-сервера.

Правила публикации веб-серверов поддерживают перенаправление HTTP-протокола в FTP-протокол. Входящий HTTP-запрос GET, сделанный к веб-прослушивателю правила публикации веб-сервера, преобразуется в FTP GET и пересылается на опубликованный FTP-сайт в сети, защищенной ОО. Таким образом, существует возможность публикации FTP-сайтов с помощью правил публикации веб-серверов.

Правила публикации прикладных серверов

Объект оценки использует механизм публикации прикладных серверов для обработки входящих запросов к различным прикладным (не-веб) ресурсам внутренней сети, таким как почтовые серверы, FTP-серверы, SQL-серверы и другие. ОО обрабатывает входящие запросы на доступ к ресурсам и в последующем переадресовывает их на внутренний сервер, расположенный за ОО в защищаемой сети.

По существу механизм публикации серверов позволяет любому компьютеру во внутренней сети осуществлять публикацию собственных ресурсов во внешних сетях. При этом безопасность данного компьютера не ставиться под угрозу вследствие того, что передача всех входящих запросов и исходящих ответов осуществляется через ОО.

Правила публикации сервера обладают следующими свойствами и возможностями.

- правила публикации сервера не обрабатывают соединения с помощью прокси;

- почти все протоколы IP-уровня и протоколы TCP/UDP можно опубликовать, применяя правила публикации сервера;
- правила публикации сервера не поддерживают аутентификацию;
- фильтрация прикладного уровня может применяться к определенному подмножеству протоколов опубликованного сервера;
- можно сконфигурировать переопределения портов для настройки ожидающих (прослушивающих) портов и переадресации портов. Можно также заблокировать использование исходных портов, запрашиваемых клиентами для соединения с опубликованным сервером;
- можно использовать IP-адрес для управления доступом к опубликованным ресурсам;
- реальный IP-адрес удаленного клиента можно сохранить или заменить IP-адресом ОО;
- имеется возможность применять расписания в правиле публикации сервера для ограничения времени доступа к опубликованному серверу;
- поддерживается переадресация портов (PAT), то есть можно получать запросы на подключение к одному порту и перенаправлять их на другой порт.

В отличие от правил публикации веб-сервера, обрабатывающих прокси-запросы к опубликованному веб-серверу, правила публикации сервера только изменяют исходный IP-адрес, прежде чем переслать запрос на соединение опубликованному серверу. Обрабатываемые прокси соединения полностью разбираются и снова компонуются ОО и таким образом предоставляют более высокую степень контроля прикладного уровня по сравнению с правилами публикации сервера.

В отличие от правил публикации веб-серверов, правила публикации прикладных серверов, могут применяться для публикации почти всех протоколов IP-уровня и TCP- или UDP-протоколов. Это существенно повышает гибкость, с которой сервисы можно сделать доступными для хостов благодаря правилам публикации сервера.

Объект оценки поставляется с набором встроенных в правила публикации определений протоколов (см. таблицу 6.1). Любой из протоколов, приведенных в таблице 6.1, готов для применения в правиле публикации сервера.

Таблица 6.1 – Определения протоколов правил публикации серверов

Определение протокола	Используемые порты	Используемые фильтры	Применение
DNS-сервер	TCP 53 входящий UDP 53 получить/ отправить	Фильтр DNS включен	Входящий протокол, используемый для публикации сервера. Это определение протокола также разрешает передачу DNS-зоны (DNS zone transfer)
Exchange RPC-сервер	TCP 135 входящий	RPC-фильтр включен	Представлены только интерфейсы (Exchange RPC UUIDs). Применяется для публикации сервера Exchange для RPC-доступа из внешней сети
FTP-сервер	TCP 21 входящий	Фильтр FTP-доступа включен	Входящий протокол, применяемый для публикации сервера. Поддерживаются режимы PASV и PORT
HTTPS-сервер	TCP 443 входящий		Входящий протокол, применяемый для публикации сервера. Используется для публикации SSL-сайтов, когда правила публикации веб-серверов и улучшенная защита не требуется
IKE-сервер	UDP 500 получить/ отправить		Входящий протокол, применяемый для публикации сервера. Используется для транзитной пересылки IPSec

Определение протокола	Используемые порты	Используемые фильтры	Применение
IMAP4-сервер	TCP 143 входящий		Входящий протокол, применяемый для публикации сервера
IMAPS-сервер	TCP 993 входящий		Входящий протокол, применяемый для публикации сервера
IPSec ESP-сервер	IP Protocol 50 получить/отправить		Входящий протокол, применяемый для публикации сервера. Используется для транзитной пересылки IPSec
IPSec NAT-T-сервер	UDP 4500 получить/ отправить		Используется для NAT-обхода (NAT Traversal) по протоколу L2TP/IPSec и других RFC-совместимых соединений с NAT-обходом для протокола IPSec
L2TP-сервер	UDP 1701 получить/ отправить		Входящий протокол, применяемый для публикации сервера. Используется для публикации управляющего канала L2TP/IPSec
Microsoft SQL-сервер	TCP 1433 входящий		Входящий протокол, применяемый для публикации сервера
MMS-сервер	TCP 1755 входящий UDP 1755 получить	MMS-фильтр включен	Входящий протокол, применяемый для публикации сервера

Определение протокола	Используемые порты	Используемые фильтры	Применение
NNTP-сервер	TCP 119 входящий		Входящий протокол, применяемый для публикации сервера
NNTPS-сервер	TCP 563 входящий		Входящий протокол, применяемый для публикации сервера
PNM-сервер	TCP 7070 входящий	PNM-фильтр включен	Входящий протокол, применяемый для публикации сервера
POP3-сервер	TCP 110 входящий		Входящий протокол, применяемый для публикации сервера
POP3S-сервер	TCP 995 входящий		Входящий протокол, применяемый для публикации сервера
PPTP-сервер	TCP 1723 входящий	PPTP-фильтр включен	Входящий протокол, применяемый для публикации сервера
RDP-сервер	TCP 3389 входящий		Входящий протокол, применяемый для публикации сервера. Используется для удаленного доступа к рабочему столу сервера
RPC-сервер (все интерфейсы)	TCP 135 входящий	RPC-фильтр включен	Входящий протокол, применяемый для публикации сервера (все RPC-интерфейсы). Прежде всего, используется для внутридоменных соединений через

Определение протокола	Используемые порты	Используемые фильтры	Применение
			ОО
RTSP-сервер	TCP 554 входящий		Входящий протокол, применяемый для публикации сервера. Используется сервисами Windows Media Server ОС Windows Server 2003
SMTP-сервер	TCP 25 входящий	SMTP-фильтр включен	Входящий протокол, применяемый для публикации сервера
SMTPS-сервер	TCP 465 входящий		Входящий протокол, применяемый для публикации сервера
Telnet-сервер	TCP 23 входящий		Входящий протокол, применяемый для публикации сервера

Один из главных недостатков правил публикации прикладного сервера по сравнению с правилами публикации веб-сервера заключается в том, что правила публикации сервера не поддерживают предварительную аутентификацию с использованием ОО. Подтверждение подлинности должно выполняться сервером, опубликованным с помощью правила публикации сервера.

Также как и правила публикации веб-серверов правила публикации серверов поддерживают проверку на прикладном уровне всех входящих и исходящих запросов через ОО с помощью следующих фильтров приложений:

- MMS-фильтр;
- PNM-фильтр;
- POP-фильтр обнаружения атак;
- PPTP-фильтр;
- RPC-фильтр;
- RTSP-фильтр;
- SMTP-фильтр;
- фильтр DNS;
- фильтр FTP-доступа;
- фильтр H.323;
- фильтр SOCKS v4;
- фильтр веб-прокси.

Данные фильтры можно условно разделить на три группы:

- фильтры доступа – используются составными протоколами для установления соединения (например, фильтр H.323, MMS-фильтр, RTSP-фильтр);
- прикладные фильтры – используются для защиты установленных через ОО соединений с помощью тестирования соответствия соединения (например, фильтр DNS, POP-фильтр обнаружения атак и RPC-фильтр);
- фильтры, которые выполняют задачи, как фильтров доступа, так и прикладных фильтров – действуют как посредники для клиентов SecureNAT в управлении составными протоколами и, кроме того, защищают соединения, для которых служат промежуточным звеном (например, фильтр SecureNAT-доступа и RPC-фильтр).

В каждом правиле публикации сервера есть возможность управлять прослушивающим или ожидающим портом, портом назначения и портом, который может

использоваться запрашивающим клиентом как исходный порт для доступа к серверу, опубликованному с помощью правила публикации сервера. В ОО правила публикации серверов позволяют переадресовывать входящие соединения на опубликованный сервер на тот же самый порт, с которого был получен исходный запрос. Такая возможность обеспечивает детальный контроль переадресации портов (отображения портов) на любом сервере, опубликованном с помощью правила публикации сервера.

Опубликованный IP-адрес компьютера в действительности является внешним IP-адресом ОО. При запросе доступа к требуемым ресурсам сервера, пользователи, запрашивающие объект, полагают, что они взаимодействуют с ОО, чье имя или IP-адрес они указали в запросе, в то время как в действительности они запрашивают информацию с опубликованного сервера.

Можно настроить правила публикации сервера для ограничения IP-адресов, которые могут соединяться с опубликованным сервером по правилу публикации сервера. При этом возможен выбор между сохранением исходного IP-адреса клиента и замещением этого адреса IP-адресом самого ОО.

Как и в правиле публикации веб-сервера в правиле публикации сервера можно включать расписание, чтобы соединения с опубликованным сервером могли устанавливаться только в указанные в расписании периоды времени, а также настроить способ пересылки соединений на опубликованный сервер и выбрать порты, используемые для доступа и пересылки запросов на соединение.

Правила доступа

Правила доступа применяются для управления соединениями между любыми двумя сетями. Существует единственное ограничение – нельзя создать правила доступа для управления соединением между сетями, использующими средства преобразования сетевых адресов (NAT), если инициирующий связь хост находится в узле сетевого соединения, не применяющего NAT.

Правила в ОО позволяют определять источник и адресат для каждого отдельного протокола, к которым разрешен доступ пользователя или группы. Это повышает гибкость при осуществлении контроля входящего и исходящего доступа через ОО. ОО позволяет контролировать доступ и применение любого протокола, включая протоколы IP-уровня.

К исходящим соединениям всегда применяются правила доступа. Только протоколы с первичным соединением в исходящем направлении или направлении отправки можно использовать в правилах доступа для исходящих соединений через ОО.

Правила доступа обеспечивают управление информационными потоками на основе следующих основных атрибутов безопасности:

- предполагаемый адрес субъекта-источника;
- предполагаемый адрес субъекта назначения;
- протокол транспортного уровня;
- интерфейс, через который осуществляется прием и передача сетевого трафика;
- запрашиваемый сервис;
- период времени;
- имя субъекта доступа (имя пользователя).

При обращении клиента (субъекта доступа) к требуемым ресурсам сети с использованием определенного протокола, ОО осуществляет проверку правила доступа. Если каждый из вышеперечисленных атрибутов безопасности совместим с одноименным атрибутами в запросе на соединение, то к соединению применяется правило доступа. В противном случае ОО отклонит запрос.

Объект оценки включает список предопределенных заранее сконфигурированных шаблонов протоколов, описывающих наиболее широко распространенные протоколы внешних сетей. При этом в ОО существует возможность добавления новых шаблонов протоколов и модификации уже имеющихся.

6.1.2.4 Фильтрация на уровне приложения

Детальная проверка с отслеживанием состояния соединения в отличие от динамической фильтрации, проверяющей информацию только на сетевом и транспортном уровнях, требует, чтобы межсетевой экран мог анализировать и принимать решения на всех коммуникационных уровнях, включая наиболее важный уровень приложений. ОО способен выполнять динамическую проверку (фильтрацию) на уровне приложений посредством веб-фильтров и фильтров приложений. Такая проверка позволяет полностью обследовать коммуникационные потоки, проходящие через ОО из одной сети в другую. Тем самым выполняется защита сети от многих современных типов угроз уровня приложения.

Веб-фильтры

Веб-фильтры (см. таблицу 6.2) используются как промежуточное звено в соединениях через ОО по протоколам HTTP, HTTPS и по туннелированному в HTTP протоколу FTP (с применением Веб-прокси). Веб-фильтры выполняют динамическую фильтрацию информации, передаваемой компонентами веб-прокси, на уровне приложений. Веб-фильтры разделяют HTTP-сообщения на составляющие и предоставляют их средствам проверки на уровне приложений.

Таблица 6.2 – Веб-фильтры, используемые в ОО

Название веб-фильтра	Описание	Направление
Фильтр приоритизированных служб	Включает разметку приоритизированными службами веб-трафика в соответствии с URL-адресом, сетью, размерами ответа и запроса	Входящие и исходящие веб-запросы
Фильтр балансировки нагрузки веб-публикации	Активирует публикацию ферм веб-серверов с балансировкой нагрузки	Входящие веб-запросы
Фильтр сжатия	Включает сжатие HTTP/HTTPS	Входящие и исходящие веб-запросы
Фильтр делегирования проверки подлинности	Включает делегирование проверки подлинности опубликованным веб-серверам	Входящие веб-запросы
Фильтр проверки подлинности на основе форм	Включает проверку подлинности на основе форм (cookie) и проверку подлинности RSA SecurID	Входящие веб-запросы
Фильтр проверки подлинности RADIUS	Включает проверку подлинности RADIUS	Входящие и исходящие веб-запросы
Фильтр проверки	Обеспечивает проверку подлинности	Входящие веб-запросы

подлинности LDAP	LDAP	
Фильтр преобразования ссылок	Включает преобразование ссылок для опубликованных веб-серверов	Входящие веб-запросы
Фильтр HTTP	Выполняет фильтрацию HTTP-трафика и вводит в действие настраиваемую политику HTTP	Входящие и исходящие веб-запросы
Фильтр кэширования сжатого содержимого	Включает кэширование сжатого содержимого HTTP	Входящие и исходящие веб-запросы

Веб-фильтры загружаются при запуске службы межсетевого экрана.

Фильтр HTTP

Фильтр HTTP – одно из ключевых средств фильтрации и проверки на прикладном уровне, включенных в состав ОО. Фильтр HTTP обеспечивает детальную проверку данных, передаваемых по протоколу HTTP, с отслеживанием состояния соединений. Фильтр HTTP позволяет контролировать практически любой аспект HTTP-соединения и блокировать или разрешать соединения, основанные на почти любом компоненте HTTP-коммуникаций.

Применение фильтра HTTP основано на правилах. Можно использовать различные параметры фильтрации в каждом правиле, разрешающем исходящие HTTP-коммуникации.

Настраиваются следующие параметры HTTP фильтрации:

- установка максимальной длины пользовательских данных;
- блокирование символов верхних битов;
- проверка нормализации;
- блокирование ответов, содержащих исполняемый контент Windows;
- настройка точно соответствующих HTTP-методов, которые нужно разрешить, и блокирование всех остальных;
- разрешение только определенного списка расширений файлов;
- разрешение только определенных заголовков запроса (request) или ответа (response);

- создание точно настроенных подписей (signatures), которые способны блокировать соединения, основываясь на URL-адресах запроса, заголовках запроса, теле запроса, заголовках ответа или теле ответа.

Возможно управлять HTTP-методами, применяемыми в правиле доступа или правиле публикации веб-сервера. HTTP-методы – это HTTP-команды, которые хосты могут посылать на веб-сервер для выполнения определенных действий, такие как GET, PUT, POST, HEAD, SEARCH, CHECKOUT и другие. Имеется три варианта по управлению HTTP-методами:

- разрешить все способы;
- разрешить только указанные способы;
- блокировать указанные способы (разрешить все остальные).

В некоторых случаях необходимо запретить пользователям запросы файлов определенных типов через ОО. Можно настроить HTTP-политику ОО так, чтобы блокировать все попытки установления соединения с исполняемыми файлами Windows независимо от расширения файла, используемого источником, либо блокировать доступ исключительно по расширению файла:

- разрешить все расширения;
- разрешить только указанные расширения;
- блокировать все указанные расширения (разрешить все остальные);
- блокировать запросы, содержащие неоднозначные расширения.

Настраиваются следующие параметры фильтрации HTTP-заголовков:

- разрешить все заголовки, кроме следующих;
- заголовок сервера;
- заголовок VIA.

Можно принимать все HTTP-заголовки или запретить конкретные, заданные HTTP-заголовки.

Можно настроить заголовок сервера, возвращаемый в HTTP-ответах. Заголовок сервера – это HTTP-заголовок, посылаемый веб-сервером обратно веб-клиенту и информирующий последнего о типе веб-сервера, с которым соединяется клиент. Имеются следующие возможности:

- отправить исходный заголовок;
- вырезать заголовок из ответа;
- изменить заголовок в ответе.

Параметр заголовок VIA позволяет управлять заголовком VIA, посылаемым веб-клиенту. Если между клиентом и веб-сервером располагаются серверы веб-прокси, то сервер веб-прокси вставляет заголовок VIA в HTTP-сообщение, информирующий клиента о том, что запрос был обработан сервером веб-прокси в процессе передачи. Каждый сервер веб-прокси на пути запроса может добавить свой собственный заголовок VIA, и каждый отправитель на пути следования ответа удаляет свой заголовок VIA и пересылает ответ на сервер, заданный в следующем заголовке VIA, хранящемся в «стеке» заголовков VIA. Имеются следующие варианты обработки заголовка VIA:

- отправить заголовок по умолчанию;
- изменить заголовок в запросе и ответе.

Установка по умолчанию на ОО – включать имя компьютера, на котором размещен ОО, в маршрутный заголовок.

Детальная проверка передачи данных по протоколу HTTP в ОО также позволяет создавать HTTP-подписи, которые могут сравниваться с URL запроса, заголовками и телом запроса, а также с заголовками и телом ответа. Это дает возможность осуществлять качественный контроль содержимого, к которому могут получить доступ внешние и внутренние пользователи через ОО.

Подпись – это цепочка символов, в поисках которой ОО проверяет тело и заголовок запроса и тело и/или заголовок ответа. Если цепочка найдена, то данные будут заблокированы. Можно выполнять поиск текстовой или битовой цепочки. Блокировка, основанная на текстовых подписях, может выполняться, только если HTTP-запросы и ответы имеют кодировку UTF-8.

Фильтр преобразования ссылок

Функциональные возможности встроенного преобразователя ссылок, а также наличие встроенного установленного по умолчанию словаря позволяют использовать его сразу после установки ОО для решения общих проблем, встречающихся в сценариях публикации веб-серверов, основанных на средствах прокси.

Установленный по умолчанию словарь преобразователя ссылок может также должным образом преобразовывать запросы к нестандартным портам.

Фильтр проверки подлинности RADIUS

Фильтр проверки подлинности RADIUS является связующим звеном для RADIUS-аутентификации клиентов веб-прокси и внешних хостов, соединяющихся с веб-сайтами, опубликованными с помощью правил публикации веб-серверов.

Фильтр проверки подлинности RADIUS применяется веб-прослушивателями, если прослушиватели настроены на использование RADIUS-аутентификации.

Фильтры приложений

Фильтры приложений (см. таблицу 6.3) отвечают за выполнение динамической фильтрации на прикладном уровне протоколов, отличных от HTTP, таких как SMTP, POP3 и DNS. Эти фильтры также разделяют сообщения на составляющие и предоставляют их для детальной динамической фильтрации на ОО.

Таблица 6.3 – Фильтры приложений, используемые в ОО

Название фильтра приложений	Описание
MMS-фильтр	Активирует протокол MMS
PNM-фильтр	Активирует протокол PNM
POP-фильтр обнаружения атак	Проверяет наличие атак переполнения буфера POP
PPTP-фильтр	Включает PPTP-туннелирование через ISA Server
RPC-фильтр	Активирует публикацию RPC-серверов
RTSP-фильтр	Активирует протокол RTSP
SMTP-фильтр	Выполняет фильтрацию SMTP-трафика
Фильтр DNS	Выполняет фильтрацию DNS-трафика
Фильтр FTP-доступа	Активирует протоколы FTP (клиент и сервер)
Фильтр H.323	Включает протокол H.323
Фильтр SOCKS v4	Активирует связь через SOCKS версии 4
Фильтр веб-прокси	Включает HTTP-прокси и кэш

Фильтры приложений обеспечивают две функции:

– доступ протокола;

– защиту протокола.

Доступ протокола обеспечивает доступ для протоколов, требующих вторичных соединений. Сложные протоколы (например, FTP или MMS) могут запросить более одного соединения через ОО, как входящего, так и исходящего. Клиенты межсетевого экрана могут использовать сложные протоколы без помощи фильтров приложений. В отличие от клиентов межсетевого экрана клиенты SecureNAT нуждаются в этих фильтрах при использовании сложных протоколов, поскольку у клиентов SecureNAT нет функциональных возможностей клиентов межсетевого экрана.

Защита протоколов – это защита соединений, проходящих через ОО. Фильтры защиты протоколов, такие как SMTP- и DNS-фильтры, проверяют соединения, применяющие эти фильтры, и блокируют те из них, которые считают не соответствующими параметрам безопасности. Некоторые из этих фильтров (такие как DNS- и SMTP-фильтры) запрещают соединения, которые могут создавать переполнения буфера, а некоторые (такие как средство просмотра сообщений SMTP Message Screener) выполняют более детальную проверку и блокируют соединения или содержимое, основываясь на политике.

Фильтры приложений могут получать доступ к потокам данных или дейтаграммам соответствующей сессии, установленной через ОО. Фильтры приложений работают с некоторыми или со всеми дейтаграммами или потоками данных протоколов прикладного уровня. Кроме того, фильтры приложений могут выполнять характерные для протокола задачи, такие как аутентификация и проверка на наличие вирусов.

MMS-фильтр

MMS-фильтр поддерживает соединения MMS через ОО с применением правил доступа и правил публикации сервера. MMS-фильтр – это фильтр доступа, позволяющий клиенту SecureNAT получить доступ к сложным протоколам и вторичным соединениям, необходимым для подключения к содержимому, хранящемуся на сервере MMS.

PNM-фильтр

PNM-фильтр поддерживает соединения по протоколу PNM. Это фильтр доступа, позволяющий клиенту SecureNAT получить доступ к сложным протоколам и вторичному соединению, необходимым для подключения к серверам PNM.

POP-фильтр обнаружения атак

POP-фильтр обнаружения атак защищает серверы POP3, опубликованные с помощью правил публикации серверов, от атак переполнения буферов POP-сервисов.

PPTP-фильтр

PPTP-фильтр поддерживает соединения по протоколу PPTP через ОО для исходящих соединений, устанавливаемых с помощью правил доступа, и входящих соединений, выполняемых с применением правил публикации сервера.

PPTP-фильтр необходим как клиентам SecureNAT, так и клиентам межсетевого экрана. В действительности компьютер, расположенный в сети, защищенной ОО, должен быть сконфигурирована как клиент SecureNAT для того, чтобы использовать PPTP-фильтр для соединения через ОО с VPN-серверами по протоколу PPTP. Причина такого подхода заключается в том, что клиент межсетевого экрана не может быть связующим звеном для протоколов, отличных от TCP/UDP.

RPC-фильтр

RPC-фильтр применяется как промежуточное звено в RPC-подключениях к серверам, требующим удаленных вызовов процедур, как для исходящих соединений, использующих правила доступа, так и для входящих соединений, применяющих правила публикации серверов. Фильтр RPC предоставляет возможность публикации RPC-серверов (например, таких как почтовый сервер Exchange), делая их доступными для внешних клиентов.

Правила публикации сервера Exchange в ОО позволяют удаленным пользователям устанавливать соединение с сервером Exchange с помощью полнофункционального клиента Outlook MAPI через внешнюю сеть. Для этого клиент Outlook должен быть настроен на использование RPC.

RPC-фильтр используется для того, чтобы не открывать порты для удаленного доступа к службам Exchange RPC с помощью клиента Outlook MAPI и не ставить безопасность под угрозу.

Фильтр RPC может быть сконфигурирован для фильтрации конкретных UUID с использованием мастера RPC, входящего в состав ОО. Он позволяет администратору выбирать с помощью мастера службы из перечня доступных на сервере интерфейсов или определять их вручную.

RTSP-фильтр

RTSP-фильтр поддерживает соединения по протоколу RTSP через ОО для правил доступа и публикации серверов. RTSP-фильтр – фильтр доступа, позволяющий клиенту SecureNAT получить доступ к сложным протоколам и вторичным соединениям, необходимым для подключения к содержимому, хранящемуся на сервере RTSP (таком как мультимедийные MMS-серверы в ОС Windows Server 2003).

SMTP-фильтр

SMTP-фильтр и средство просмотра сообщений SMTP Message Screener (не входит в ОО) применяются для защиты опубликованных SMTP-серверов. SMTP-фильтр защищает опубликованные SMTP-серверы от атак переполнения буфера, а средство просмотра сообщений защищает от нежелательных сообщений электронной почты. Кроме того, фильтр SMTP может быть сконфигурирован на прием или отклонение определенных SMTP-команд, а также на прием команд только установленной длины.

Фильтр DNS

Фильтр DNS защищает DNS-сервер, опубликованный с помощью правил публикации сервера.

После включения функции обнаружение вторжения и DNS-атак можно активизировать защиту от трех видов DNS-атак:

- переполнение имен узлов DNS;
- переполнение длины DNS;
- передачи зон DNS.

Фильтр FTP-доступа

Фильтр FTP-доступа применяется как посредник в FTP-соединениях между клиентами защищенной сети и FTP-серверами во внешней сети, а также между внешними хостами и опубликованными FTP-серверами. Фильтр FTP-доступа поддерживает режимы PASV и PORT (пассивный и стандартный, или активный) FTP-соединений.

Фильтр FTP-доступа необходим для клиентов SecureNAT, поскольку протокол FTP использует вторичные соединения для FTP-соединений в режиме PORT. Протокол FTP – сложный протокол, требующий исходящих соединений от FTP-клиента в режиме PORT и новых вторичных входящих соединений от FTP-сервера.

Можно настроить FTP-политику ОО так, чтобы разрешить пользователям загружать и размещать файлы по протоколу FTP или же можно ограничить FTP-доступ пользователя только загрузкой. Это дает возможность более тщательного контроля обмена данными по протоколу FTP и лучшего обеспечения безопасности.

Фильтр FTP-доступа является более функциональным, чем определяемый пользователем протокол FTP, потому что он динамически открывает конкретные порты для дополнительного подключения и может выполнять преобразование адресов, необходимое для дополнительного подключения. Этот фильтр также может различать разрешения на чтение и запись, что дает возможность более точного контроля доступа.

Фильтр H.323

Фильтр H.323 применяется для поддержки соединений H.323.

Фильтр SOCKS v4

Фильтр SOCKS v4 используется для приема запросов на соединения SOCKS версии 4 от приложений, разработанных в соответствии со спецификацией SOCKS версии 4. В операционных системах семейства Windows нет необходимости применять фильтр SOCKS, поскольку можно установить клиент межсетевого экрана на этих компьютерах для прозрачной аутентификации на ОО и поддержки взаимодействия сложных протоколов.

На хостах, которые нельзя конфигурировать как клиенты межсетевого экрана, таких как Linux- и Mac-хосты, можно использовать для поддержки фильтр SOCKS v4. По умолчанию этот фильтр отключен. Однако в работе клиента SOCKS и клиента межсетевого экрана есть существенные отличия.

Рекомендуется применять клиент межсетевого экрана, потому что он обладает значительными преимуществами, предоставляя возможность подтверждения подлинности всех Winsock-соединений, устанавливаемых через ОО. Однако SOCKS – это подходящий, лучший из оставшихся, вариант, если нельзя установить клиент межсетевого экрана.

Фильтр веб-прокси

Фильтр веб-прокси позволяет перенаправлять в кэш или на компоненты веб-прокси соединения от хостов, не конфигурированных как клиенты веб-прокси. Если требуется,

чтобы только хосты, настроенные явно как клиенты веб-прокси, использовали функциональные возможности веб-прокси, можно отсоединить фильтр веб-прокси.

6.1.2.5 Сетевые шаблоны

В ОО имеются сетевые шаблоны, которые можно использовать для облегчения процесса конфигурирования политики межсетевого экрана по управлению трафиком между несколькими сетями.

Эти шаблоны включают следующие наиболее распространенные схемы сетей:

- пограничный межсетевой экран – используется для подключения внутренней сети к внешним сетям и защиты внутренней сети от несанкционированного доступа;
- трехзонная конфигурация сервера – используется для подключения внутренней сети к внешним сетям, защиты внутренней сети от несанкционированного доступа, а также для публикации служб во внешних сетях из демилитаризованной зоны;
- внешний межсетевой экран – используется, если имеется два межсетевых экрана между защищенной внутренней сетью и внешней сетью. ОО используется как передняя линия защиты в конфигурации демилитаризованной зоны с двумя межсетевыми экранами;
- внутренний межсетевой экран – используется, если имеется два межсетевых экрана между защищенной внутренней сетью и внешней сетью. ОО используется как внутренняя линия защиты в конфигурации демилитаризованной зоны с двумя межсетевыми экранам;
- одна сетевая плата – используется внутри внутренней сети или демилитаризованной зоны, если ОО будет использоваться для веб-прокси, кэширования, веб-публикации или публикации сервера веб-клиента Outlook.

Вместе с шаблоном поставляются политики межсетевого экрана, которые становятся доступными при запуске шаблона. Рекомендуется выбрать политику «Блокировать все», а затем настроить ее с конкретными правилами доступа и правилами публикации для конкретной организации.

6.1.2.6 Режим блокировки

Режим блокировки ОО обеспечивает защиту ФБО и ресурсов подключенных к нему сетей в случае, если в результате атаки будут отключены службы межсетевого экранирования.

Каждый раз, когда возникает ситуация, вследствие которой службы межсетевого экранирования прекращают свою работу, ОО переходит в режим блокировки. Когда ОО находится в режиме блокировки, всегда применяется ограниченная совокупность правил системной политики.

Режим блокировки активируется:

- когда сетевая атака или другое событие в сети или на локальном хосте вызовет отключение служб межсетевого экранирования, например из-за ошибки или ситуации, когда пользователь намеренно настраивает оповещения и действия при оповещении таким образом, что службы межсетевого экранирования отключаются в ответ на событие, которое спровоцировало это оповещение;
- когда службы межсетевого экранирования отключаются вручную. Также можно отключить службы межсетевого экранирования для эффективной реакции на атаку в случае, когда в процессе конфигурирования ОО и сети становится известно о ее подготовке.

При переходе в режим блокировки ОО сохраняет следующие функции:

- механизм пакетной фильтрации ОО применяет политику режима блокировки ОО;
- правила политики доступа разрешают исходящий трафик из сети локального хоста ко всем сетям (если они так настроены). Если устанавливается исходящее соединение, то это соединение может использоваться для ответа на входящий трафик. Например, DNS-ответ на DNS-запрос может быть принят по одному соединению. Это не означает, что режим блокировки разрешает расширить существующую политику для исходящего доступа из сети локального хоста. Допустимы только существующие правила, разрешающие исходящий доступ из сети локального хоста;
- новые первичные соединения с самим ОО разрешаются только в том случае, когда включено правило системной политики, которое разрешает именно такой трафик. Исключением является DHCP-трафик, который разрешен всегда.

DHCP-запросы (на порт UDP 67) разрешены из сети локального хоста во все сети, а DHCP-ответы (на порт UDP 68) разрешены в обратном направлении;

- VPN-клиенты удаленного доступа не смогут устанавливать соединение с ОО. VPN-соединения «узел-в-узел» также будут запрещены;
- любые изменения в конфигурации сети в режиме блокировки применяются только после перезапуска служб межсетевого экранирования и выходе из режима блокировки ОО;
- ОО не будет инициировать никаких оповещений.

6.1.2.7 Поддержка защищенных соединений

Для предоставления стандартного безопасного удаленного доступа используются встроенные службы виртуальных частных сетей Microsoft® Windows® 2000 и Microsoft® Windows® Server 2003. Объект оценки поддерживает безопасные VPN-подключения филиалов или удаленных пользователей к основному офису. Политика межсетевого экрана применяется к VPN-подключениям и позволяет точно контролировать протоколы и ресурсы, к которым получают доступ пользователи таких подключений.

Сопоставление с ФТБ

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

- FDP_IFC.1 – ФБО осуществляют политику управления информационными потоками для субъектов – сущностей ИТ внешних и внутренней (защищаемой ОО) сетей, информации – сетевого трафика, передающегося через ОО между субъектами, операций – запросов к сервисам, перемещения информации (в том числе пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств);
- FDP_IFF.1 – ФБО осуществляют политику управления информационными потоками, основанную на определенных атрибутах безопасности, перемещение информации через ОО осуществляется в строгом соответствии с правилами, устанавливаемыми на ОО;
- FPT_RCV.1 – ФБО обеспечивают наличие процедур, предоставляющих возможность возврата ОО к безопасному состоянию после сбоя или прерывания обслуживания;

– FTP_ITC.1 – ФБО обеспечивают поддержку установления защищенных соединений с обеспечением конфиденциальности и целостности передаваемой информации.

6.1.3 Функции безопасности «Управление безопасностью»

Объект оценки позволяет настроить три уровня контроля программного обеспечения ОО в зависимости от роли, назначенной пользователю.

На ОО предусмотрены следующие административные роли:

- аудитор ISA Server – пользователи и группы, которым назначена эта роль, могут выполнять мониторинг работы ОО и сети, но не могут настраивать функции мониторинга;
- аудитор наблюдения ISA Server – пользователи и группы, которым назначена эта роль, могут выполнять все типы мониторинга, включая конфигурирование журналов, оповещений и других функций, разрешенных для этой роли;
- полный администратор ISA Server – пользователи и группы, которым назначена эта роль, могут выполнять любые настройки на ОО, включая конфигурирование правил, применение сетевых шаблонов и мониторинг.

Пользователи, которым назначены эти роли, могут быть созданы в локальном диспетчере учетных записей безопасности SAM операционной системы Microsoft Windows Server 2003 SP1, под управлением которой функционирует ОО, или это могут быть пользователи домена, если ОО является членом домена Active Directory внутренней сети. ОО позволяет выполнять проверку подлинности пользователей в Active Directory и в других аутентификационных базах данных, используя службу RADIUS для отправки запросов к Active Directory.

Административные роли ОО могут быть назначены любым пользователям, для этого не нужны никакие особые права или полномочия. Исключением является случай, когда пользователю нужно выполнять мониторинг счетчиков производительности ОО с помощью монитора производительности ISA Server или инструментальной панели ОО. В таком случае пользователь должен быть членом группы пользователей журналов производительности операционной системы, под управлением которой функционирует ОО.

По умолчанию роль полного администратора ISA Server назначена администратору и группе администраторы из локального диспетчера учетных записей безопасности SAM операционной системы, под управлением которой функционирует ОО.

Делегирование прав контроля программного обеспечения ОО позволяет предоставлять пользователям, не имеющим административной роли на ОО, делегировать (передавать) определенные административные функции. Данный подход обеспечивает распределение административных задач среди соответствующих групп пользователей.

Существует возможность контроля входящего и исходящего доступа по пользователям, группам, приложениям, источникам и местам назначения, по изменению контента, а также по расписанию. С помощью мастеров политик межсетевого экрана задаются доступные веб-сайты и контент, доступность определенного протокола для установки входящих и исходящих подключений, а также разрешения на установку подключений между определенными IP-адресами с помощью заданных протоколов и портов.

Конфигурацию межсетевого экрана можно целиком скопировать в файл XML и передать администратору другого межсетевого экрана, чтобы обеспечить стандартную конфигурацию в рамках всей организации. Из этого файла можно также импортировать отдельные элементы конфигурации.

Управлять работой ОО можно в удаленном режиме с помощью следующих не входящих в ОО средств:

- оснастки MMC;
- служб терминалов Windows 2000;
- удаленного рабочего стола Windows Server 2003.

Кроме того, удаленное управление службами ОО возможно с помощью сценариев, запускаемых из командной строки. Графические панели задач и мастера конфигурации упрощают навигацию и настройку стандартных задач.

Можно создавать оповещения на основе событий и использовать их для запуска и остановки служб межсетевого экрана, а также автоматического выполнения действий на основании заданных критериев.

Сопоставление с ФТБ

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

- FMT_MSA.1 – ФБО обеспечивают возможность добавления правил, удаления правил, модификации атрибутов в правилах политики управления информационными потоками только уполномоченному администратору ОО;
- FMT_MSA.3 – ФБО обеспечивают ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики управления информационными потоками и возможность для уполномоченного администратора ОО определять альтернативные значения для отмены значений по умолчанию;
- FMT_SMR.1 – ФБО поддерживает ролевую модель, определяя роль администратора 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 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, в которых описываются действия по выполнению функций безопасности ОО и приводятся предупреждения уполномоченным администраторам 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 отображения соответствия функций

безопасности, представленных в функциональной спецификации, функциям безопасности, идентифицированным в краткой спецификации.

Сопоставление с ТДБ

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

– ADV_FSP.1;

– ADV_RCR.1.

6.2.4 Тестирование

Корпорация Microsoft® 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 «Материалы анализа стойкости функций безопасности Microsoft® Internet Security and Acceleration Server™ 2006 Standard Edition».

Сопоставление с ТДБ

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

– AVA_SOF.1.

7 Утверждения о соответствии ПЗ

Утверждения о соответствии профилям защиты отсутствуют.

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.NetFiltration	O.TrsptFiltration	O.ApplFiltration	O.RegisterFiltration	O.LocalAlarm	O.RegisterAdmEnter	O.RegisterStartPrg	O.RegisterFeatures	O.DisasterRecovery	O.AdminManage	O.SecurConnect	O.IntruderDetect
T.UnauthAccess	X	X	X									
T.AuditOverflow								X				
T.MaliciousFailure									X			
P.NetFiltration	X											
P.TrsptFiltration		X										
P.ApplFiltration			X									
P.RegisterFiltration				X								
P.LocalAlarm					X							
P.RegisterAdmEnter						X						
P.RegisterStartPrg							X					
P.AuditFinder								X				
P.Manage										X		

	O.NetFiltration	O.TrsptFiltration	O.ApplFiltration	O.RegisterFiltration	O.LocalAlarm	O.RegisterAdmEnter	O.RegisterStartPrg	O.RegisterFeatures	O.DisasterRecovery	O.AdminManage	O.SecurConnect	O.IntruderDetect
P.SecurConnect											X	
P.IntruderDetect												X

O.NetFiltration

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.UnauthAccess** и реализацией политики безопасности организации **P.NetFiltration**, так как обеспечивает осуществление фильтрации ОО на сетевом уровне на основе сетевых адресов отправителя и получателя, а также с учетом даты и времени, а также осуществление возможности по фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств, по фильтрации с учетом входного и выходного сетевого интерфейса, и по фильтрации с учетом любых значимых полей сетевых пакетов.

O.TrsptFiltration

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.UnauthAccess** и реализацией политики безопасности организации **P.TrsptFiltration**, так как обеспечивает осуществление фильтрации на транспортном уровне запросов на установление виртуальных соединений на основе транспортных адресов отправителя и получателя, а также с учетом даты и времени.

O.ApplFiltration

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.UnauthAccess** и реализацией политики безопасности организации **P.ApplFiltration**, так как обеспечивает фильтрации на прикладном уровне запросов к прикладным сервисам на основе прикладных адресов отправителя и получателя, а также с учетом даты и времени.

O.RegisterFiltration

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.RegisterFiltration**, так как обеспечивает возможность регистрации и учета фильтруемых пакетов, а также запросов на установление виртуальных соединений; в параметры регистрации включаются адрес, время и результат фильтрации.

O.LocalAlarm

Достижение этой цели безопасности необходимо в связи с с реализацией политики безопасности организации **P.LocalAlarm**, так как обеспечивает возможность локальной сигнализации попыток нарушения правил фильтрации.

O.RegisterAdmEnter

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.RegisterAdmEnter**, так как обеспечивает регистрацию входа (выхода) администратора ОО в систему (из системы) либо загрузки и инициализации системы и ее программного останова, при этом в параметрах регистрации указываются дата, время и код регистрируемого события, результат попытки осуществления регистрируемого события, идентификатор администратора ОО, предъявленный при попытке осуществления регистрируемого события.

O.RegisterStartPrg

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.RegisterStartPrg**, так как обеспечивает возможность регистрации запуска программ и процессов (заданий, задач).

O.RegisterFeatures

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.AuditOverflow** и реализацией политики безопасности организации **P.AuditFinder**, так как обеспечивает наличие средств сортировки и поиска событий аудита на основе заданных атрибутов, а также невозможность потери записей аудита вследствие недостаточности выделенного объема дискового пространства.

O.DisasterRecovery

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.MaliciousFailure**, так как обеспечивает возможность восстановления после сбоев и отказов оборудования, предусматривающую восстановление свойств ОО.

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, доступных только уполномоченным администраторам ОО.

O.SecurConnect

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.SecurConnect**, так как обеспечивает поддержку установления защищенных соединений (с обеспечением целостности и конфиденциальности передаваемой информации) с внешними доверенными системами.

O.IntruderDetect

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.IntruderDetect**, так как обеспечивает возможность обнаружения наиболее распространенных форм сетевых вторжений при взаимодействии внутренней (защищаемой ОО) сети с внешними сетями.

8.1.2 Обоснование целей безопасности для среды

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

Таблица 8.2 – Отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности организации

	OE.NonWiretapAuth	OE.AccessAdm	OE.RemovedQuery	OE.RegisterAdmAction	OE.ControlIntegrity	OE.ImpossibleModif	OE.TOEConfig	OE.LocateTOE	OE.QualifyAdm	OE.Environment	OE.GenerateTime	OE.ProtectFileSystem
A.ImpossibleModif						X						
A.TOEConfig							X					
A.LocateTOE								X				
A.QualifyAdm									X			
TE.WiretapAuthQuery	X											
TE.WiretapAuthAdm			X									
TE.MaliciousIntegrity					X							
P.AccessAdm		X										
P.RegisterAdmAction				X								
P.Environment										X		
P.GenerateTime											X	
P.ProtectFileSystem												X

OE.NonWiretapAuth

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **TE.WiretapAuthQuery**, так как обеспечивает возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

OE.AccessAdm

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.AccessAdm**, так как обеспечивает идентификацию и аутентификацию администратора ОО при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия, при этом

осуществляется препятствование доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

OE.RemovedQuery

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **TE.WiretapAuthAdm**, так как обеспечивает, при удаленных запросах администратора ОО на доступ, идентификацию и аутентификацию методами, устойчивыми к пассивному и активному перехвату информации.

OE.RegisterAdmAction

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.RegisterAdmAction**, так как обеспечивает регистрацию действий администратора ОО по изменению правил фильтрации.

OE.ControlIntegrity

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **TE.MaliciousIntegrity**, так как обеспечивает контроль целостности программной и информационной части ОО по контрольным суммам.

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.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 исключение возможности несанкционированного физического доступа к компьютеру с установленным ОО.

OE.QualifyAdm

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.QualifyAdm**, так как обеспечивает благонадежность и компетентность персонала, ответственного за администрирование ОО, который руководствуется в своей деятельности соответствующей документацией.

OE.Environment

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Environment**, так как обеспечивает функционирование ОО в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.GenerateTime

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.GenerateTime**, так как обеспечивает поддержку средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

OE.ProtectFileSystem

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.ProtectFileSystem**, так как обеспечивает защиту программного обеспечения и конфигурационных фалов ОО на уровне файлов файловой системы ОС от несанкционированного доступа.

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.NetFiltration	O.TrsptFiltration	O.ApplFiltration	O.RegisterFiltration	O.LocalAlarm	O.RegisterAdmEnter	O.RegisterStartPrg	O.RegisterFeatures	O.DisasterRecovery	O.AdminManage	O.SecurConnect	O.IntruderDetect
FAU_ARP.1					X							X
FAU_GEN.1 (1)				X		X	X					
FAU_SAA.1					X							X
FAU_SAR.1								X				
FAU_SAR.3								X				
FAU_STG.4								X				
FDP_IFC.1	X	X	X									
FDP_IFF.1	X	X	X									
FMT_MSA.1										X		
FMT_MSA.3										X		
FMT_SMR.1										X		
FPT_RCV.1									X			
FTP_ITC.1											X	

FAU_ARP.1 Сигналы нарушения безопасности

Выполнение требований данного компонента обеспечивает возможность осуществления действий по локальной сигнализации попыток нарушения правил

фильтрации. Рассматриваемый компонент сопоставлен с целями **O.LocalAlarm, O.IntruderDetect** и способствует их достижению.

FAU_GEN.1 (1) Генерация данных аудита безопасности

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с целями **O.RegisterFiltration**, **O.RegisterAdmEnter**, **O.RegisterStartPrg** и способствует их достижению.

FAU_SAA.1 Анализ потенциального нарушения

Выполнение требований данного компонента обеспечивает возможность применения набора правил мониторинга событий, подвергающихся аудиту, и указаний на возможное нарушение ПБО, основываясь на этих правилах. Осуществляется накопление или объединение известных событий, связанных с фильтрацией информации, указывающих на возможное нарушение безопасности. Рассматриваемый компонент сопоставлен с целями **O.LocalAlarm, O.IntruderDetect** и способствует их достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления администратору ОО всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **O.RegisterFeatures** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение фильтрации, поиска и сортировки данных аудита, основанных на определенных критериях (времени, адресе отправителя, адресе получателя, порте, действии). Рассматриваемый компонент сопоставлен с целью **O.RegisterFeatures** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает выполнение записи новых данных аудита поверх самых старых хранимых записей аудита при отсутствии

свободного дискового пространства для создания журнала аудита. Рассматриваемый компонент сопоставлен с целью **O.RegisterFeatures** и способствует ее достижению.

FDP_IFC.1 Ограниченное управление информационными потоками

Выполнение требований данного компонента обеспечивает реализацию политики управления информационными потоками для субъектов, информации и операций запросов к сервисам, а также перемещения информации (в том числе пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств). Рассматриваемый компонент сопоставлен с целями **O.NetFiltration**, **O.TrsptFiltration**, **O.ApplFiltration** и способствует их достижению.

FDP_IFF.1 Простые атрибуты безопасности

Выполнение требований данного компонента обеспечивает осуществление политики управления информационными потоками, основываясь на атрибутах безопасности, определении правил фильтрации. Рассматриваемый компонент сопоставлен с целями **O.NetFiltration**, **O.TrsptFiltration**, **O.ApplFiltration** и способствует их достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента предусматривает возможность добавления правила, удаления правила, модификации атрибутов в политики управления информационными потоками, только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики управления информационными потоками, и возможность для уполномоченного администратора ОО определять альтернативные значения для отмены значений по умолчанию. 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 роли администратора ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FPT_RCV.1 Ручное восстановление

Выполнение требований данного компонента обеспечивает, что после сбоя или прерывания обслуживания ФБО перейдут в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию. Рассматриваемый компонент сопоставлен с целью **O.DisasterRecovery** и способствует ее достижению.

FTP_ITC.1 Доверенный канал передачи между ФБО

Выполнение требований данного компонента обеспечивает предоставление канала связи между ФБО и удаленным доверенным продуктом ИТ, который логически отличим от других каналов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту данных канала от модификации или раскрытия. Рассматриваемый компонент сопоставлен с целью **O.SecurConnect** 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 ОО). В части 3 ОК ОУД1 определен, как предусматривающий функциональное тестирование.

Выбор ОУД1 в качестве пакета требований доверия в настоящем ЗБ осуществлен исходя из необходимости получения определенной уверенности в правильном функционировании ОО и независимого подтверждения, что уделяется должное внимание защите конфиденциальной информации со стороны разработчика, а также с учетом стоимости и длительности реализации и оценки выполнения этих требований и отсутствия необходимости предоставления и анализа представления реализации (исходных текстов) ОО.

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 требований безопасности для среды ИТ

В таблице 8.4 представлено отображение функциональных требований безопасности среды ИТ на цели безопасности для среды.

Таблица 8.4 – Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	OE.NonWiretapAuth	OE.AccessAdm	OE.RemovedQuery	OE.RegisterAdmAction	OE.ControlIntegrity	OE.Environment	OE.GenerateTime	OE.ProtectFileSystem
FAU_GEN.1 (2)				X				
FAU_STG.1								X
FIA_AFL.1		X				X		
FIA_SOS.1		X				X		
FIA_UAU.2		X						
FIA_UAU.8 (EXT)	X							
FIA_UAU.9 (EXT)			X					
FIA_UID.2		X						
FPT_AMT.1					X			
FPT_SEP.1								X
FPT_STM.1							X	
FPT_TST.1					X			

FAU_GEN.1 (2) Генерация данных аудита безопасности

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО (действий администратора ОО по изменению правил фильтрации). Рассматриваемый компонент сопоставлен с целью **OE.RegisterAdmAction** 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 **OE.ProtectFileSystem** и способствует ее достижению.

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает блокировку регистрационной записи субъекта доступа при превышении установленного числа неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целями **OE.AccessAdm**, **OE.Environment** и способствует их достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает верификацию качества паролей на доступ к ОО. Рассматриваемый компонент сопоставлен с целями **OE.AccessAdm**, **OE.Environment** и способствует их достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает, что администратор ОО при его локальных запросах на доступ должен быть успешно аутентифицирован по паролю условно-постоянного действия до разрешения любого действия, выполняемого при посредничестве ФБО от имени администратора ОО. Рассматриваемый компонент сопоставлен с целью **OE.AccessAdm** и способствует ее достижению.

FIA_UAU.8 (EXT) Аутентификация запросов

Выполнение требований данного компонента обеспечивает, возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети. Рассматриваемый компонент сопоставлен с целью **OE.NonWiretapAuth** и способствует ее достижению.

FIA_UAU.9 (EXT) Аутентификация при удаленном доступе

Выполнение требований данного компонента обеспечивает, возможность идентификации и аутентификации методами, устойчивыми к пассивному и активному

перехвату информации при удаленных запросах администратора ОО на доступ. Рассматриваемый компонент сопоставлен с целью **OE.RemovedQuery** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает, чтобы каждый администратор ОО при его локальных запросах на доступ успешно идентифицировался по идентификатору (коду) до разрешения любого действия, выполняемого при посредничестве ФБО от имени администратора ОО. Рассматриваемый компонент сопоставлен с целями **OE.AccessAdm** и способствует ее достижению.

FPT_AMT.1 Тестирование абстрактной машины

Выполнение требований данного компонента обеспечивает выполнение пакета тестовых программ по запросу уполномоченного администратора ОО для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая является базовой для ФБО. Рассматриваемый компонент сопоставлен с целью **OE.ControlIntegrity** 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 **OE.ProtectFileSystem** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ЗБ для удовлетворения зависимости компонентов FAU_GEN.1 (1) и FAU_GEN.1 (2) от наличия в записях аудита точного указания даты и времени. Рассматриваемый компонент сопоставлен с целью **OE.GenerateTime** и способствует ее достижению.

FPT_AMT.1 Тестирование абстрактной машины

Выполнение требований данного компонента обеспечивает выполнение пакета программ тестирования ФБО периодически в процессе нормального функционирования

для демонстрации правильного выполнения ФБО, целостность данных ФБО и целостность хранимого выполняемого кода ФБО верифицируется по контрольным суммам. Рассматриваемый компонент сопоставлен с целью **OE.ControlIntegrity** и способствует ее достижению.

8.2.3 Обоснование зависимостей требований

В таблице 8.5 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 8.5 является справочным и содержит компоненты, определенные в части 2 ОК в описании компонентов требований, приведенных в столбце 1 таблицы 8.5, под рубрикой «Зависимости».

Столбец 3 таблицы 8.5 показывает, какие компоненты требований были реально включены в настоящий ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 8.5. Компоненты требований в столбце 3 таблицы 8.5 либо совпадают с компонентами в столбце 2 таблицы 8.5, либо иерархичны по отношению к ним.

Таблица 8.5 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
Зависимости функциональных требований ОО		
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1
FAU_GEN.1 (1)	FPT_STM.1	FPT_STM.1
FAU_SAA.1	FAU_GEN.1	FAU_GEN.1 (1)
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1 (1)
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, FMT_MSA.3

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RCV.1	FPT_TST.1, AGD_ADM.1, ADV_SPM.1	FPT_TST.1, AGD_ADM.1, *обосновано невключение ADV_SPM.1*
Зависимости функциональных требований среды ИТ		
FAU_GEN.1 (2)	FPT_STM.1	FPT_STM.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1 (1), FAU_GEN.1 (2)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FPT_TST.1	FPT_AMT.1	FPT_AMT.1

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

Включение в ЗБ компонента FPT_RCV.1 требует для удовлетворения зависимостей включения компонента ADV_SPM.1, однако разработчиком в руководствах ОО

предоставлено четкое определение безопасного состояния ФБО, при котором ФБО не противоречивы и продолжают корректное осуществление ПБО и объяснение, почему такое состояние можно считать безопасным, в связи с этим, зависимость компонента FPT_RCV.1 от компонента ADV_SPM.1 не учитывается.

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

8.3 Обоснование краткой спецификации ОО

Обоснование краткой спецификации ОО представлено таблицей 8.6 и таблицей 8.7.

Таблица 8.6 – Отображение функциональных требований безопасности на функции безопасности

	Аудит безопасности	Защита данных пользователя	Управление безопасностью
FAU_ARP.1	X		
FAU_GEN.1 (1)	X		
FAU_SAA.1	X		
FAU_SAR.1	X		
FAU_SAR.3	X		
FAU_STG.4	X		
FDP_IFC.1		X	
FDP_IFF.1		X	
FMT_MSA.1			X
FMT_MSA.3			X
FMT_SMR.1			X
FPT_RCV.1		X	
FTP_ITC.1		X	

Таблица 8.7 – Отображение требований доверия на меры безопасности

	Управление конфигурацией	Предоставление руководств	Предоставление проектной документации	Тестирование
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

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 средней СФБ в качестве уровня стойкости функций безопасности обосновывается предназначением ОО (межсетевое экранирование) и является достаточным (в соответствии с руководящим документом ФСТЭК (Гостехкомиссии) России «Безопасность информационных технологий. Руководство по формированию семейств профилей защиты») для определения допустимости использования ОО при обработке конфиденциальной информации.

Приложение А

Соответствие требованиям Руководящего документа ФСТЭК (Гостехкомиссии) России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации», предъявляемым к межсетевым экранам четвертого класса защищенности

В данном Приложении демонстрируется соответствие ОО (с учетом среды функционирования) требованиям Руководящего документа ФСТЭК (Гостехкомиссии) России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации», предъявляемым к межсетевым экранам четвертого класса защищенности (см. таблицу А.1).

Таблица А.1 – Соответствие требованиям Руководящего документа ФСТЭК (Гостехкомиссии) России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (РД МЭ), предъявляемым к межсетевым экранам четвертого класса защищенности.

Требования 4 класса защищенности РД МЭ	Реализации требований	
	ОО	**Среда функционирования**
1. УПРАВЛЕНИЕ ДОСТУПОМ		
1.1 Фильтрация на сетевом уровне. Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов. 1.2 Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств. 1.3 Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов. 1.4 Фильтрация с учетом любых значимых полей сетевых пакетов.	FDP_IFC.1, FDP_IFF.1	
2. РЕГИСТРАЦИЯ		
2.1 Возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.	FAU_GEN.1 (1)	
3. АДМИНИСТРИРОВАНИЕ: ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ		
3.1 Идентификация и аутентификация администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.		FIA_UAU.2, FIA_UID.2

Требования 4 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
4. АДМИНИСТРИРОВАНИЕ: РЕГИСТРАЦИЯ		
4.1 Регистрация входа (выхода) администратора МЭ в систему (из системы) либо загрузка и инициализация системы и ее программный останов. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ; В параметрах регистрации указываются: − дата, время и код регистрируемого события; − результат попытки осуществления регистрируемого события – успешная или неуспешная; − идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события. 4.2 Регистрация запуска программ и процессов (заданий, задач)	FAU_GEN.1 (1)	
5. ЦЕЛОСТНОСТЬ		
5.1 МЭ должен содержать средства контроля за целостностью своей программной и информационной части.		FPT_TST.1, FPT_AMT.1
6. ВОССТАНОВЛЕНИЕ		
6.1 МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.	FPT_RCV.1	

Требования 4 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
7. ТЕСТИРОВАНИЕ		
7.1 В МЭ должна обеспечиваться возможность регламентного тестирования: − реализации правил фильтрации (см. п. 1); − процесса регистрации (см. п. 2); − процесса идентификации и аутентификации администратора МЭ (см. п. 3); − процесса регистрации действий администратора МЭ (см. п. 4); − процесса контроля за целостностью программной и информационной части МЭ (см. п. 5); − процедуры восстановления (см. п.6).		FPT_TST.1, FPT_AMT.1
8. РУКОВОДСТВО АДМИНИСТРАТОРА МЭ		
8.1 Документ должен содержать: − описание контролируемых функций МЭ; − руководство по настройке и конфигурированию МЭ; − описание старта МЭ и процедур проверки правильности старта; − руководство по процедуре восстановления.	AGD_ADM.1	
9. ТЕСТОВАЯ ДОКУМЕНТАЦИЯ		
9.1 Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 7.1), и результаты тестирования.	ATE_IND.1	

Требования 4 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
10. КОНСТРУКТОРСКАЯ (ПРОЕКТНАЯ) ДОКУМЕНТАЦИЯ		
10.1 Должна содержать: − общую схему МЭ; − общее описание принципов работы МЭ; − описание правил фильтрации; − описание средств и процесса идентификации и аутентификации; − описание средств и процесса регистрации; − описание средств и процесса контроля за целостностью программной и информационной части МЭ; − описание процедуры восстановления свойств МЭ.	ADV_FSP.1	

Приложение Б

Соответствие требованиям Руководящего документа ФСТЭК (Гостехкомиссии) России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации», предъявляемым к межсетевым экранам третьего класса защищенности

В данном Приложении демонстрируется соответствие ОО (с учетом среды функционирования) требованиям Руководящего документа ФСТЭК (Гостехкомиссии) России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации», предъявляемым к межсетевым экранам третьего класса защищенности (см. таблицу Б.1).

Таблица Б.1 – Соответствие требованиям Руководящего документа ФСТЭК (Гостехкомиссии) России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (РД МЭ), предъявляемым к межсетевым экранам третьего класса защищенности.

Требования 3 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
1. УПРАВЛЕНИЕ ДОСТУПОМ		
10.2Фильтрация на сетевом уровне. Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов. 10.3Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств. 10.4Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов. 10.5Фильтрация с учетом любых значимых полей сетевых пакетов. 10.6Фильтрация на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя. 10.7Фильтрация на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя. 10.8Фильтрация с учетом даты/времени.	FDP_IFC.1, FDP_IFF.1	
2. АУТЕНТИФИКАЦИЯ		
2.1 Возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.		FIA_UAU.8 (EXT)

Требования 3 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
3. РЕГИСТРАЦИЯ		
3.1 Возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.	FAU_GEN.1 (1)	
3.2 Регистрация и учет запросов на установление виртуальных соединений.	FAU_GEN.1 (1)	
3.2 Локальная сигнализация попыток нарушения правил фильтрации.	FAU_ARP.1, FAU_SAA.1	
4. АДМИНИСТРИРОВАНИЕ: ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ		
4.1 Идентификация и аутентификация администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.		FIA_UAU.2, FIA_UID.2
4.2 Препятствование доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.		FIA_AFL.1
4.3 При удаленных запросах администратора МЭ на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.		FIA_UAU.9 (EXT)

Требования 3 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
5. АДМИНИСТРИРОВАНИЕ: РЕГИСТРАЦИЯ		
5.1 Регистрация входа (выхода) администратора МЭ в систему (из системы) либо загрузка и инициализация системы и ее программный останов. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ; В параметрах регистрации указываются: − дата, время и код регистрируемого события; − результат попытки осуществления регистрируемого события – успешная или неуспешная; − идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события. 5.2 Регистрация запуска программ и процессов (заданий, задач)	FAU_GEN.1 (1)	
5.3 Регистрация действия администратора МЭ по изменению правил фильтрации.		FAU_GEN.1 (2)
6. АДМИНИСТРИРОВАНИЕ: ПРОСТОТА ИСПОЛЬЗОВАНИЯ		
6.1 Многокомпонентный МЭ должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.	ОО является однокомпонентным МЭ	
7. ЦЕЛОСТНОСТЬ		
7.1 МЭ должен содержать средства контроля за целостностью своей программной и информационной части. 7.2 Должен обеспечиваться контроль целостности программной и информационной части МЭ по контрольным суммам.		FPT_TST.1, FPT_AMT.1

Требования 3 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
8. ВОССТАНОВЛЕНИЕ		
8.1 МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.	FPT_RCV.1	
9. ТЕСТИРОВАНИЕ		
9.1 В МЭ должна обеспечиваться возможность регламентного тестирования: − реализации правил фильтрации (см. п. 1); − процесса регистрации (см. п. 3); − процесса идентификации и аутентификации запросов (см. п. 2); − процесса идентификации и аутентификации администратора МЭ (см. п. 4); − процесса регистрации действий администратора МЭ (см. п. 5); − процесса контроля за целостностью программной и информационной части МЭ (см. п. 7); − процедуры восстановления (см. п.8).		FPT_TST.1, FPT_AMT.1
10. РУКОВОДСТВО АДМИНИСТРАТОРА МЭ		
10.1 Документ должен содержать: − описание контролируемых функций МЭ; − руководство по настройке и конфигурированию МЭ; − описание старта МЭ и процедур проверки правильности старта; − руководство по процедуре восстановления.	AGD_ADM.1	

Требования 3 класса защищенности РД МЭ	Реализации требований	
	ОО	Среда функционирования
11. ТЕСТОВАЯ ДОКУМЕНТАЦИЯ		
11.1 Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 9.1), и результаты тестирования.	ATE_IND.1	
12. КОНСТРУКТОРСКАЯ (ПРОЕКТНАЯ) ДОКУМЕНТАЦИЯ		
12.1 Должна содержать: − общую схему МЭ; − общее описание принципов работы МЭ; − описание правил фильтрации; − описание средств и процесса идентификации и аутентификации; − описание средств и процесса регистрации; − описание средств и процесса контроля за целостностью программной и информационной части МЭ; − описание процедуры восстановления свойств МЭ. 12.2 Должна содержать описание средств и процесса централизованного управления компонентами МЭ.	ADV_FSP.1	