**ЛЕКЦИЯ 7. Технология Microsoft обеспечения информационной безопасности**

Процесс обеспечения безопасности относится к оперативным процессам и, в соответствии с библиотекой ITIL, входит в блок процессов поддержки ИТ-сервисов. Нарушение безопасности информационной системы предприятия может привести к ряду негативных последствий, влияющих на уровень предоставления ИТ-сервисов:

* снижение уровня доступности вследствие отсутствия доступа или низкой скорости доступа к данным, приложениям или службам;
* полная или частичная потеря данных;
* несанкционированная модификация данных;
* получение доступа посторонних пользователей к конфиденциальной информации.

Анализ причин нарушения информационной безопасности показывает, что основными являются следующие:

* ошибки конфигурирования программных и аппаратных средств ИС;
* случайные или умышленные действия конечных пользователей и сотрудников ИТ-службы;
* сбои в работе программного и аппаратного обеспечения ИС;
* злоумышленные действия посторонних по отношению к информационной системе лиц.

Компания Microsoft разрабатывает стратегию построения защищенных информационных систем (Trustworthy Computing) - это долгосрочная стратегия, направленная на обеспечение более безопасной, защищенной и надежной работы с компьютерами для всех пользователей.

Концепция защищенных компьютерных систем построена на четырех принципах:

* *безопасность*, которая предполагает создание максимально защищенных ИТ-инфраструктур;
* *конфиденциальность*, которая подразумевает внедрение в состав и технологий и продуктов средств защиты конфиденциальности на протяжении всего периода их эксплуатации;
* *надежность*, которая требует повышения уровня надежности процессов и технологий разработки программного обеспечения информационных систем;
* *целостность деловых подходов* для укрепления доверия клиентов, партнеров, государственных учреждений.

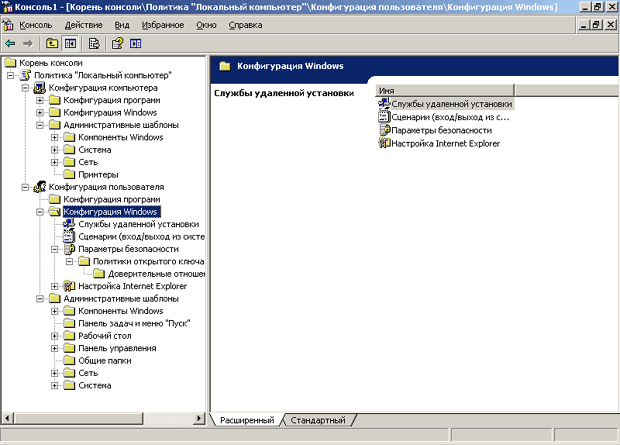
Данные принципы реализуются в программных продуктах Microsoft. Компания Microsoft предлагает обеспечивать безопасность операционных систем семейства Windows с помощью технологии единого каталога (Active Directory) и групповых политик. Использование групповой политики и Active Directory позволяет централизовано управлять параметрами безопасности как для одного пользователя или компьютера, так и для группы пользователей, управлять безопасностью серверов и рабочих станций.

Для решения вопросов обеспечения информационной безопасности компания Microsoft предоставляет следующие технологии:

* Active Directory – единый каталог, позволяющий сократить число паролей, которые должен вводить пользователь;
* двухэтапная аутентификация на основе открытых/закрытых ключей и смарт-карт;
* шифрование трафика на базе встроенных средств операционной системы IPSec (IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов);
* создание защищенных беспроводных сетей на основе стандарта IEEE 802.1x;
* шифрование файловой системы;
* защита от вредоносного кода;
* организация безопасного доступа мобильных и удаленных пользователей;
* защита данных на основе кластеризации, резервного копирования и ограничения несанкционированного доступа;
* служба сбора событий из системных журналов безопасности.

**7.1 Групповые политики**

Управление групповыми политиками в Microsoft Windows Server 2003 позволяет администраторам задавать конфигурацию операционных систем серверов и клиентских компьютеров. Реализуется эта функциональность с помощью оснастки "Редактор объектов групповой политики", общий вид которой приведен на рис. 7.1.

[](http://www.intuit.ru/EDI/21_12_14_1/1419110295-31391/tutorial/406/objects/7/files/07_01.png)

**Рис. 7.1.** Оснастка "Редактор объектов групповой политики"

Для компьютеров, входящих в домен Active Directory, используются групповые политики, определяющие политики безопасности, используемые в рамках сайта, домена или набора организационных единиц (OU – organizational units).

Групповые политики и Active Directory позволяют:

* централизованно управлять пользователями и компьютерами в масштабах предприятия;
* автоматически применять политики информационной безопасности;
* понижать сложность административных задач (например, обновление операционных систем, установка приложений);
* унифицировать параметры безопасности в масштабах предприятия;
* обеспечить эффективную реализацию стандартных вычислительных средств для групп пользователей.

При управлении безопасностью информационной системы предприятия групповая политика позволяет управлять контроллерами доменов и серверами, определять наборы параметров для конкретной группы пользователей, параметры защиты, сетевой конфигурации и ряд других параметров, применяемых к определенной группе компьютеров.

Active Directory позволяет управлять через групповые политики любыми службами и компонентами на платформе Windows.

Групповые политики Active Directory позволяют администраторам централизованно управлять ИТ-инфраструктурой предприятия. С помощью групповой политики можно создавать управляемую ИТ-инфраструктуру информационной системы. Эти возможности позволяют снизить уровень ошибок пользователей при модификации параметров операционных систем и приложений, а также совокупную стоимость владения информационной системы, связанную с администрированием распределенных сетей.

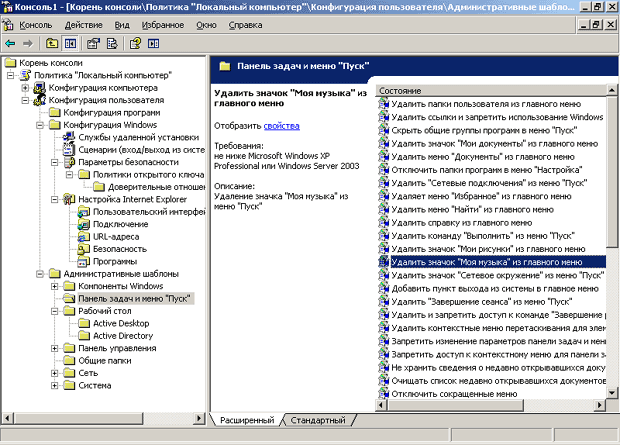
Групповая политика позволяет создать ИТ-инфраструктуру предприятия, ориентированную на потребности пользователей, сформированных в строгом соответствии с их должностными обязанностями и уровнем квалификации.

Применение групповых политик и Active Directory для сайтов, доменов и организационных единиц необходимо реализовывать с учетом следующих правил:

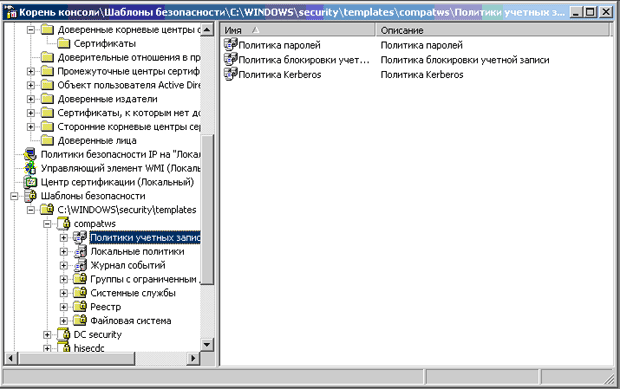
* объекты групповой политики (GPO) хранятся в каждом домене индивидуально;
* с одним сайтом, доменом или организационной единицей может быть сопоставлено несколько GPO;
* с нескольких сайтов, доменов или организационных единиц могут использовать единственную GPO;
* любому сайту, домену или организационной единице можно сопоставить любую GPO;
* параметры, определяемые GPO, можно фильтровать для конкретных групп пользователей или компьютеров на основе их членства в группах безопасности или с помощью WMI-фильтров.

При администрировании ИТ-инфраструктуры предприятия администраторы посредством механизма групповой политики могут производить настройку приложений, операционных систем, безопасность рабочей среды пользователей и информационных систем в целом. Для этого используются следующие возможности:

* политика на основе реестра. С помощью редактора объектов групповой политики можно задать параметры в реестре для приложений, операционной системы и её компонентов (например, администратор может удалить из главного меню значок "Моя музыка", что представлено на рис. 7.2.);
* параметры безопасности. Администраторы могут указывать параметры локальной, доменной и сетевой защиты для компьютеров и пользователей в области действия GPO, используя шаблоны безопасности (рис. 7.3);

[](http://www.intuit.ru/EDI/21_12_14_1/1419110295-31391/tutorial/406/objects/7/files/07_02.png)

**Рис. 7.2.** Удаление значка из главного меню профиля пользователя

[](http://www.intuit.ru/EDI/21_12_14_1/1419110295-31391/tutorial/406/objects/7/files/07_03.png)

**Рис. 7.3.** Оснастка Политика учетных записей шаблонов безопасности

* ограничения на использование программ. Данные ограничения предназначены для защиты от вирусов, выполнения нежелательных программ и атак на компьютеры;
* распространение и установка программ. Обеспечивается возможность централизованного управления установкой, обновлением и удалением приложений;
* сценарии для компьютеров и пользователей. Данные средства позволяют автоматизировать операции, выполняемые при запуске и выключении компьютера, при входе и выходе пользователя;
* мобильные пользовательские профили и перенаправление папок. Профили хранятся на сервере и позволяют загружаться на тот компьютер, где пользователь входит в систему. Перенаправление папок позволяет размещать важные для пользователя папки на сервере;
* автономные папки. Данный механизм позволяет создавать копии сетевых папок, синхронизировать их с сетью и работать с ними при отключении сети;
* поддержка Internet Explorer. Эта возможность позволяет администраторам проводить управление конфигурацией Microsoft Internet Explorer на компьютерах с поддержкой групповой политики.

Для общего контроля применения групповой политики используются механизм WMI – фильтров (Windows Management Instrumentation). Данное решение позволяет администраторам создавать и модифицировать WMI – запросы для фильтрации параметров безопасности, определяемых групповыми политиками. WMI – фильтры позволяют динамически задавать область действия групповой политики на основе атрибутов целевого компьютера.

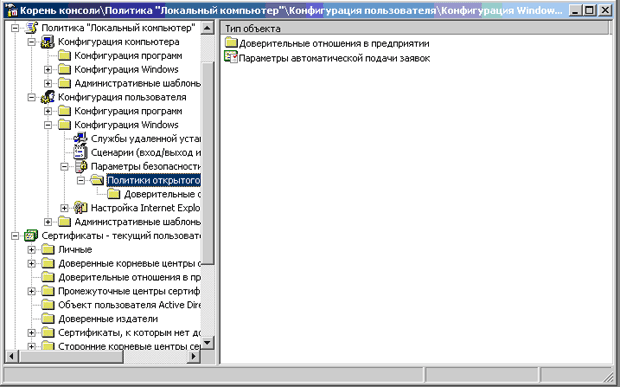
Применение механизма групповой политики для ИТ-инфраструктуры предприятия способствует снижению сложности решения задач развертывания обновлений, установки приложений, настройки профилей пользователей и, в целом, администрирования информационной системы. Применение групповой политики в информационной системе предприятия дает следующие преимущества:

* повышение эффективности использования инфраструктуры Active Directory;
* повышение гибкости выбора области администрирования для предприятий, различающихся по размеру и отраслевой принадлежности, при происходящих изменениях в бизнесе;
* наличие интегрированного средства управления групповой политикой на основе консоли GPMC;
* простота в использовании, которая обеспечивается удобным и понятным пользовательским интерфейсом консоли GPMC, что приводит к сокращению расходов на обучение и повышает эффективность труда администраторов;
* надежность и безопасность действий администраторов за счет автоматизации процесса ввода групповых политик в действие;
* централизованное управление конфигурациями на основе стандартизации пользовательских вычислительных сред.

**7.2 Безопасный доступ в сеть**

ИТ-инфраструктура предприятия может включать интрасети, сайты в интернете и экстрасети. Многие компоненты такой инфраструктуры являются потенциально уязвимыми перед попытками неавторизованного доступа со стороны злоумышленников. Контроль и управление идентификацией пользователей может быть осуществлен на базе инфраструктуры открытых ключей.

Инфраструктура открытых ключей PKI (public key infrastructure) – это системы цифровых сертификатов, центров сертификации CA (certification authorities) и других центров регистрации RA (registration authorities), которые идентифицируют (проверяют подлинность) каждой стороны, участвующей в электронной транзакции, с применением шифрования открытым ключом (public key). В Microsoft Server 2003 политику открытых ключей можно задавать с помощью оснастки MMC - Политика открытого ключа (рис. 7.4.)

[](http://www.intuit.ru/EDI/21_12_14_1/1419110295-31391/tutorial/406/objects/7/files/07_04.png)

**Рис. 7.4.** Оснастка Политика открытого ключа

В Windows Server 2003 центр сертификации предполагает применение электронных цифровых подписей. Службы сертификации (Certification Services) и средства управления сертификатами позволяют построить предприятию собственную инфраструктуру открытых ключей.

Применение инфраструктуры открытых ключей обеспечивает следующие преимущества для информационной системы предприятия:

* *более устойчивая к взлому защита*, которая базируется на аутентификации с высокой степенью защищенности и применении смарт-карт, использовании протокола IPSec для поддержания целостности и защиты данных от попыток несанкционированной модификации при передаче по общедоступным сетям, а также использовании шифрующей файловой системы для защиты конфиденциальных данных, хранящихся на сервере;
* *упрощение администрирования* за счет создания сертификатов, которые позволяют избавиться от применения паролей, масштабировать доверительные отношения в рамках предприятия;
* *дополнительные возможности*, которые обеспечивают безопасный обмен файлами и данными между сотрудниками предприятия по общедоступным сетям, защищенную электронную почту и безопасное соединение через Web;
* *использование сертификатов*, которые представляют собой цифровой документ, выпускаемый центром сертификации и подтверждающий идентификацию владельца данного сертификата. Сертификат связывает открытый ключ с идентификацией лица, компьютера или службы, которые имеют соответствующий закрытый ключ;
* *службы сертификации*, которые применяются при создании и управлении центрами сертификации. В корпоративной информационной системе может быть один или несколько центров сертификации, которые управляются через оснастку Центр сертификации консоли MMC;
* *шаблоны сертификатов*, которые представляют собой набор правил и параметров, применяемых к входящим запросам на сертификаты определенного типа;
* *автоматическая подача заявок на сертификаты*, которая позволяет администратору конфигурировать субъекты сертификатов для автоматического запроса сертификатов, получения выданных сертификатов и возобновления просроченных сертификатов без участия их субъектов;
* *Web-страницы подачи заявок на сертификаты*, которые позволяют подавать заявки на сертификаты через Web-браузер;
* *политики открытых ключей*, которые позволяют автоматически распространять сертификаты их субъектам, определять общие доверяемые центры сертификации и проводить управление политиками восстановления данных;
* *поддержка смарт-карт*, которая позволяет обеспечивать вход в систему через сертификаты на смарт-картах, хранение на них сертификатов и закрытых ключей. Смарт-карты предназначены для обеспечения безопасности аутентификации клиентов, входа в домен под управлением Windows Server, цифрового подписания программного кода, работы с защищенной электронной почтой на основе применения шифрования с открытыми ключами.

**7.3 Аутентификация пользователей**

В операционной системе Windows Server 2003 применяются следующие стандартные протоколы аутентификации:

* *интерактивный ввод*, при котором идентификация пользователя проверяется по учетной записи на локальном компьютере или в Active Directory;
* *аутентификация* в сети предполагает идентификацию пользователя любой сетевой службой, к которой обращается пользователь, с использованием протокола Kerberos V5, сертификатов открытых ключей, SSL (Security Sockets Layer) и TLS-кэш (Transport Layer Security);
* единый вход, который дает возможность обращаться к сетевым ресурсам без повторного ввода учетных данных.

В Windows Server 2003 поддерживается аутентификация с применением смарт-карт, что позволяет создавать корпоративные сети с высоким уровнем защищенности. Смарт-карта – это устройство внешне похожее на кредитную карту, на котором хранятся пароли, открытые и закрытые ключи и другие личные данные пользователя.

Для активизации смарт-карты пользователь должен вставить её в устройство чтения, подключенное к компьютеру, и ввести свой PIN-код (персональный идентификационный номер). PIN-код обрабатывается локально и не передается по сети. После нескольких неудачных попыток ввода PIN-кода смарт-карта блокируется.

Ввод PIN-кода обеспечивает аутентификацию только по отношению к смарт-карте, а не к домену. Для аутентификации в домене применяется сертификат открытого ключа, хранящийся на смарт-карте. При запросе на вход сначала происходит обращение к локальной системе безопасности клиентского компьютера. Далее происходит обращение к службе аутентификации домена с использованием сертификата пользователя. Удостоверение сертификата подтверждается цифровой подписью с применением закрытого ключа пользователя.

**7.4 Защита коммуникаций**

Для защиты коммуникаций предназначена технология IP-безопасности, базирующаяся на протоколе IPSec (IP Security). В корпоративной информационной системе данная технология должна обеспечивать защиту от:

* изменения данных при пересылке;
* перехвата, просмотра и копирования данных;
* несанкционированного изменения определенных ролей в системе;
* перехвата и повторного использования пакетов для получения доступа к конфиденциальным ресурсам.

Протокол IPSec представляет протокол транспортного уровня с защитой данных на основе шифрования, цифровой подписи и алгоритмов хеширования. Он обеспечивает безопасность на уровне отдельных IP-пакетов, что позволяет защищать обмен данными в общедоступных сетях и обмен данными между приложениями, не имеющими собственных средств безопасности.

IPSec в Windows Server 2003 интегрирован с политиками безопасности Active Directory, что обеспечивает хорошую защищенность интрасетей и коммуникаций через Internet.

В IPSec предусмотрены криптографические механизмы хеширования и шифрования для предупреждения атак. Протокол имеет следующие средства защиты:

* аутентификация отправителя на основе цифровой подписи;
* проверка целостности данных на основе алгоритмов хеширования;
* использование алгоритмов шифрования DES и 3DES;
* защита от воспроизведения пакетов;
* свойство неотрекаемости (nonrepudiat ion), которое предполагает применение цифровой подписи для однозначного доказательства авторства сообщения;
* динамическая генерация ключей при передаче данных;
* алгоритм согласования ключей Диффи-Хелмана, который позволяет согласовывать ключ, не передавая его по сети;
* возможность задавать длину ключей.

При передаче данных с одного компьютера на другой по протоколу IPSec согласовывается уровень защиты, используемый в сеансе. В процессе согласования определяются методы аутентификации, хеширования, возможно туннелирования и шифрования. Секретные ключи для аутентификации создаются на каждом компьютере локально на основе информации, которой они обмениваются. Эта информация не передается по сети. После создания ключа выполняется аутентификация и инициируется сеанс защищенного обмена данными.

**7.5 Защита от вторжений и вредоносного ПО**

Защита от вторжений должна обеспечить профилактические меры по защите компьютеров и данных. Эти задачи решает Microsoft ISA (Internet Security and Acceleration) Server 2004. ISA Server 2004 включает межсетевой экран прикладного уровня, поддержку виртуальных частных сетей (Virtual Public Netware – VPN), Web-кэширование, фильтры прикладного уровня. ISA Server 2004 защищает корпоративные информационные системы от внутренних и внешних атак. Сервер выполняет динамическую проверку потока данных и расширенную фильтрацию различных протоколов Интернета на прикладном уровне, что позволяет противостоять угрозам, не обнаруживаемым традиционными межсетевыми экранами. ISA Server 2004 позволяет:

* защитить периметр сети;
* увеличить скорость доступа к Интернету за счет кэширования Web-страниц;
* обеспечить безопасную публикацию Web-сервисов IIS;
* предоставлять доступ VPN-клиентам к ресурсам сети и сервисам, в случае исполнения роли сервера VPN;
* объединять локальные сети через VPN-соединение, в случае исполнения роли шлюза VPN;
* расширить возможности мониторинга и регистрации VPN-соединений, позволяя отслеживать и сохранять трафик на уровне отдельных приложений;
* составлять отчеты, используя встроенные средства;
* фильтровать пакеты для всех сетевых интерфейсов;
* осуществлять поддержку туннельного режима IPSec для VPN-подключений "точка – точка";
* поддерживать режим Windows Quarantine (сетевой карантин), что повышает безопасность работы удаленных пользователей;
* поддерживать произвольную топологию и неограниченное количество сетей.

Сервер Microsoft ISA Server 2004 реализует функциональные возможности трехуровневого межсетевого экрана, средства управления частными виртуальными сетями и службы Web-кэширования. ISA Server 2004 позволяет повысить безопасность и производительность корпоративной информационной сети, а также снизить эксплуатационные расходы. Сервер ISA Server 2004 имеет ряд достоинств:

* *более совершенные средства защиты*, которые реализуют динамическую фильтрацию пакетов и каналов. Алгоритм динамической фильтрации избирательно открывает доступ пакетов данных в защищенные области сети. По мере необходимости служба динамической фильтрации открывает порты, а по завершению сеанса связи – закрывает;
* *простота использования* за счет поддержки многоуровневой архитектуры, унификации управления VPN, понятных шаблонов, усовершенствованных средств устранения неполадок, возможности экспорта конфигурации в форматах XML, мониторинга активных соединений в режиме реального времени;
* *быстрое и надежное получение доступа* к виртуальной частной сети за счет встроенной поддержки туннельного режима IPSec для VPN-подключений, быстрое Web-кэширование и высокопроизводительный пакетный фильтр.

Задачи безопасности, а также надежности, масштабируемости, быстродействия при управлении Web-серверами обеспечиваются полнофункциональным Web-сервером Internet Information Services (IIS) 6.0. Службы IIS 6.0 базируются на архитектуре обработки запросов, которая реализует среду с изоляцией приложений. Это обеспечивает функционирование отдельных Web-приложений в собственном Web-процессе. При таком режиме работа приложений и сайтов реализуется обособлено рабочими процессами, полностью изолированными от ядра Web-сервера, что исключает их влияние друг на друга.

В IIS 6.0 включены разнообразные средства управления для администрирования и конфигурирования ИТ-инфраструктуры предприятия. Системные администраторы могут изменять параметры и отлаживать приложения во время работы служб. Службы IIS 6.0 поддерживают стандарты XML, SOAP и IPv6.

Для защиты от вирусов корпоративных информационных систем Microsoft предлагает технологию Microsoft Antigen, которая позволяет защитить серверы поддержки коммуникаций и коллективной работы. Эти решения серверного уровня предоставляют средства фильтрации файлов и контента, а также позволяют применять несколько механизмов сканирования одновременно. Комплекс антивирусных средств Microsoft Antigen помогают обеспечить антивирусную защиту на уровне серверов с использованием нескольких механизмов сканирования.

Продукты семейства Antigen - это приложения для серверов коллективной работы и передачи сообщений, которые обеспечивают защиту от атак злоумышленников, вирусов и нежелательных сообщений.

Использование многоядерной технологии антивирусного сканирования позволяет продуктам Antigen успешно бороться с возникающими угрозами.

Тесная интеграция с Microsoft Exchange Server, Microsoft SharePoint и Microsoft Live Communications Server обеспечивает надежную защиту и централизованное управление всей системой защиты без снижения производительности серверов, на которых установлены продукты Antigen.

Фильтрация содержания и файлов обеспечивает соблюдение единой корпоративной политики по правилам передачи и хранения документов, а также применения допустимой лексики как внутри компании, так и при отправке сообщений поставщикам и клиентам.

Продукты семейства Antigen имеют следующие преимущества:

* *многоуровневая защита*, которая обеспечивает выбор необходимых антивирусных ядер защиты различных модулей и уровней для обеспечения максимальной защиты ИТ-инфраструктуры предприятия;
* *оптимизация сервера*, позволяющая в зависимости от роли сервера, его загрузки и мощности можно выбрать оптимальный вариант защиты – количество ядер, используемых для проверки на различных уровнях;
* *контроль содержания*, что поддерживает формировании единой корпоративной политики по правилам передачи и хранения документов, а также возможность исключить применение недопустимой лексики при передаче сообщений между подразделениями и при отправке сообщений за пределы предприятия.

Решения Microsoft для обеспечения повышенной защиты от компьютерных атак и воздействия вредоносного ПО включают следующие продукты:

* Windows Defender (бета-версия 2) предназначено для компьютерной защиты. Оно помогает блокировать "всплывающие" браузерные окна и пресекает деятельность программ-шпионов (spyware);
* Microsoft Client Protection (MCP) помогает защитить настольные компьютеры, портативные ПК и серверы от внезапных внешних сетевых угроз;
* Certificate Lifecycle Manager- решение на основе анализа бизнес-процессов, помогающее предприятиям управлять жизненным циклом цифровых сертификатов и смарт-карт;
* Windows Malicious Software Removal Tool (MSRT) - выполняет проверку системы и удаляет самое распространенное вредоносное ПО в случае его обнаружения;
* Windows OneCare \text{\texttrademark}Live содержит антивирусный модуль, брандмауэр, систему резервного копирования и восстановления данных и другие средства защиты.

В табл. 7.1. и 7.2. приведены ресурсы по обеспечению безопасности ИТ- инфраструктуры корпоративных систем.

|  |  |  |
| --- | --- | --- |
| Таблица 7.1. Русскоязычные ресурсы по обеспечению безопасности | | |
| **Наименование ресурса** | | **Web-ссылка** |
| Ресурс Microsoft, посвященный безопасности | | <http://www.microsoft.com/rus/security> |
| Центр рекомендаций по обеспечению безопасности для пользователей | | <http://www.microsoft.com/rus/securityguidance> |
| Рекомендации по обеспечению безопасности для ИТ-специалистов | | <http://www.microsoft.com/rus/technet/security> |
| Сайт Security at Home для клиентов | | <http://www.microsoft.com/rus/athome/security> |
| Сайт программы Malicious Software Removal Tool | | <http://www.microsoft.com/rus/security/malwareremove/default.mspx> |
| Сведения о системах Windows и Linux | | <http://www.microsoft.com/rus/getthefacts> |
| Таблица 7.2. Англоязычные ресурсы по обеспечению безопасности | | |
| **Наименование ресурса** | **Web-ссылка** | |
| Ресурс о безопасности для разработчиков ПО | <http://www.msdn.microsoft.com/security> | |
| Ресурсы по обеспечению безопасности для партнеров | <https://partner.microsoft.com/security> | |
| Пакет обновления 1 (SP1) для Windows Server 2003 | <http://www.microsoft.com/windowsserver2003/downloads/servicepacks/spl> | |
| Пакет обновления 1 (SP1) для Windows XP | <http://www.microsoft.com/athome/security/protect/windowsxp/choose.mspx> | |
| Microsoft Windows Defender (бета-версия 2) | <http://www.microsoft.com/athome/security/spyware/software> | |
| Стратегия Microsoft по борьбе с программами-шпионами | <http://www.microsoft.com/athome/security/spyware/strategy.mspx> | |
| Критерии Microsoft для определения программ-шпионов | <http://www.microsoft.com/athome/security/spyware/software/isv> | |
| Система Microsoft Antigen | <http://www.microsoft.com/windowsserversystern/solutions/security/sybari.mspx> | |
| Обеспечение безопасности всего цикла разработки | <http://www.msdn.microsoft.com/security/sdl> | |
| Исследовательский центр Microsoft Security Response Center | <http://www.microsoft.com/security/msrc> | |
| Microsoft Windows OneCare Live (бета-версия) | <https://beta.windowsonecare.com> | |
| Центр интернет-обслуживания Windows Live Safety Center (бета-версия) | <http://www.safety.live.com> | |

**7.6 Безопасность мобильных пользователей корпоративных систем**

Для обеспечения сотрудников постоянным доступом к ресурсам корпоративной сети в неё включают мобильные устройства. С помощью мобильных устройств сотрудники предприятия могут обращаться к корпоративной информации, своей почте и бизнес-приложениям с любого места, находящегося за межсетевым экраном корпоративной сети. Для поддержки мобильных пользователей необходимо реализовать в системе стандарты безопасности, позволяющие использовать корпоративные сетевые ресурсы и конфиденциальную информацию.

Для безопасной работы мобильных пользователей используются следующие виды защиты:

* защита домена;
* защита мобильного устройства;
* защита беспроводных соединений.

При *защите домена* мобильные устройства должны отвечать требованиям аутентификации, применяемым на предприятии. Устройства, работающие под управлением Windows Mobile 2003, поддерживают двухэтапную аутентификацию и позволяют применять стойкие пароли, биометрические технологии и сертификаты. Устройства с Windows Mobile 2003 можно интегрировать в существующую инфраструктуру открытых ключей.

*Защиту мобильных устройств*, работающих под управлением Windows Mobile 2003, поддерживают средства защиты, которые позволяют защищать информацию, хранящуюся на таких устройствах. Это предотвращает несанкционированный доступ к данным в случае утери или кражи мобильного устройства. В Windows Mobile 2003 в дополнение к поддержке строгих паролей встроены средства шифрования данных.

Для *защиты беспроводных соединений* сетевые администраторы должны контролировать процесс доступа этих устройств к корпоративной сети предприятия. Кроме того, информация, передаваемая по беспроводной сети должна шифроваться.

Одним из решений по организации доступа сотрудников, находящихся вне предприятия, к корпоративной сети является организация виртуальной частной сети – VPN. Для контроля доступа к приложениям в Windows Server 2003 имеется служба сетевого карантина (Windows Quarantine). Карантин используется в сети для проверки состояния клиента пред тем, как предоставить ему доступ к защищенным сетям. Карантинный фильтр на основании политики безопасности может запретить доступ и не разрешать его до тех пор, пока настройки подключаемого компьютера не будут удовлетворять требованиям политики безопасности. Для применения карантина требуется, чтобы эта служба поддерживалась и клиентом, и сервером аутентификации.

Некоторые мобильные устройства, такие как КПК и смартфоны, работающие под управлением Windows Mobile 2003, имеют возможность синхронизации данных. Эти мобильные устройства оптимизированы для синхронизации с серверами Microsoft Exchange. Для синхронизации данных Exchange КПК и смартфоны, управляемые Windows Mobile могут использовать Exchange Server 2003 ActiveSync. На каждом устройстве с Windows Mobile указывают сервер Exchange и задают параметры безопасности. Для соединения с сетью, в которой работает Exchange Server 2003 ActiveSync, мобильное устройство должно иметь информацию по учетной записи пользователя и имени доступных серверов. Это позволяет создать шифруемый канал коммуникационной связи между мобильным пользователем и корпоративной сетью.

**7.7 Службы терминалов**

Сервер терминалов (Terminal Server) операционной системы Windows Server 2003 позволяет с удаленных клиентских компьютеров получить через сеть доступ к приложениям, установленным на сервере. Сервер терминалов обеспечивает шифрование канала связи. Для аутентификации соединений со службами терминалов и шифрования коммуникаций с сервером терминалов применяется Secure Sockets Layer (SSL) / Transport Layer Security (TLS).

SSL – протокол шифрованной передачи данных между клиентом и сервером, который требует сертификата, выданного одним из авторизованных центров. TLS - криптографический протокол, который обеспечивает безопасную передачу данных между узлами в сети Internet. Различие между SSL 3.0 и TLS 1.0 незначительные, поэтому далее в тексте термин "SSL" будет относиться к ним обоим. SSL, используя криптографию, предоставляет возможности аутентификации и безопасной передачи данных через Internet. Часто происходит лишь аутентификация сервера, в то время как клиент остается неаутентифицированным. Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытых ключей

SSL включает в себя три основных фазы:

* диалог между сторонами, целью которого является выбор алгоритма шифрования;
* обмен ключами на основе криптосистем с открытым ключом или аутентификация на основе сертификата;
* передача данных, шифруемых при помощи симметричных алгоритмов шифрования.

Для корректной работы аутентификации SSL (TLS) удаленные клиенты должны:

* работать под управлением Windows 2000 или Windows XP;
* использовать клиент протокола RDP (Remote Desktop Protocol);
* доверять корневому сертификату сервера.

**7.8 Защита данных**

Для защиты данных применяются технологии кластеризации, теневого копирования, а также службы управления правами и Data Protection Manager.

*Кластер* определяет группу компьютеров, которые совместно выполняют одинаковый набор приложений и которые представляются клиентам и приложениям как единая система. Компьютеры объединяются в кластер с помощью программных соединений и используют средства автоматического восстановления после сбоев и балансировки сетевой нагрузки.

Windows Server 2003 имеет две службы кластеризации:

* *служба кластеров* (Cluster Service, MSCS), которая обеспечивает высокую отказоустойчивость и масштабируемость для баз данных, коммуникационных систем, файловых служб и служб печати. В системе реализуется режим автоматического восстановления после сбоя, при котором в случае недоступности одного узла кластера обработку начинает проводить другой узел;
* служба балансировки сетевой нагрузки (Network Load Balancing Service, NLBS), которая обеспечивает балансировку нагрузки, создаваемую IP-трафиком, между кластерами. Служба NLBS повышает отказоустойчивость и масштабируемость приложений, размещаемых на серверах в Internet (Web-серверах, серверах, передающих потоковую информацию, служб терминалов).

Интеграция служб кластеризации с Active Directory позволяет проводить регистрацию в Active Directory "виртуального" объекта компьютера, поддерживать аутентификацию через Kerberos и обеспечивать тесную интеграцию с другими службами, публикующими информацию о себе в Active Directory.

*Теневое копирование* общих папок в Windows Server 2003 помогает предотвратить случайную потерю данных и обеспечивает экономичный способ восстановления данных, утраченных в результате ошибки пользователя. При теневом копировании регулярно, через заданный интервал времени, создаются теневые копии файлов и папок, хранящиеся в общих сетевых папках. Теневая копия представляет предыдущую версию файла или папки по состоянию на определенный момент времени.

Посредством теневых копий файловый сервер под управлением Windows Server 2003 может эффективно поддерживать на выбранных томах предыдущие версии всех файлов. Пользователь имеет возможность просматривать предыдущие версии файла.

Теневые копии упрощают текущее восстановление поврежденных файлов, но они не заменяют процедуры резервного копирования, создания архивов, полнофункциональной системы восстановления данных.

Теневые копии не обеспечивают защиту от потери данных при сбоях или повреждении физического носителя. Тем не менее восстановление данных из теневых копий уменьшает количество случаев, в которых приходится прибегать к восстановлению данных из архивов.

Следует отметить, что теневые копии не предназначены для использования в качестве средств управления версиями документов. Это временные копии, автоматически создаваемые по расписанию.

Microsoft System Center *Data Protection Manager* (DPM) предназначен для резервного копирования на диск. DPM обеспечивает постоянную эффективную защиту данных, быстрое и надежное их восстановление. Это реализуется путем использования репликации, а также инфраструктуры службы теневого копирования томов

Резервное копирование с использованием DPM может быть централизованным (копирование по схеме "диск-диск-лента в центре обработки данных") и децентрализованным (резервные копии передаются на центральный сервер DPM).

При восстановлении данных могут выполняться следующие сценарии:

* полное восстановление сервера администраторами сервера;
* восстановление файлов администраторами сервера;
* восстановление файлов ИТ-службой;
* восстановление файлов самими пользователями.

В заключении следует отметить, что компания Microsoft разработала программное средство для оценки системы безопасности Security Assessment Tool (MSAT). Данный инструментарий позволяет собирать данные о системе безопасности ИТ-инфраструктуры предприятия и получать рекомендации по её усовершенствованию.

В данной теме была рассмотрена стратегия, технологии и решения компании Microsoft по построению защищенных информационных систем.

**7.9 Вопросы для самопроверки**

1. К каким негативным последствиям, влияющим на уровень предоставления ИТ-сервисов, могут привести нарушение безопасности информационной системы предприятия?
2. Назовите основные причины нарушения информационной безопасности для предприятия.
3. Какие технологии предоставляет Microsoft для решения вопросов обеспечения информационной безопасности?
4. Что позволяют обеспечить групповые политики и Active Directory в плане информационной безопасности предприятия?
5. С учетом каких правил необходимо применять групповые политике и Active Directory для сайтов, доменов и организационных единиц?
6. Какие возможности механизма групповой политики используются при администрировании ИТ-инфраструктуры предприятия при настройке приложений, операционных систем, безопасности рабочей среды пользователей и информационных систем в целом?
7. Для чего используются WMI – фильтры?
8. Какие преимущества дает применение групповой политики в информационной системе предприятия ?
9. Поясните назначение инфраструктуры открытых ключей PKI.
10. Какие преимущества для информационной системы предприятия дает применение инфраструктуры открытых ключей?
11. Какие стандартные протоколы аутентификации применяются в операционной системе Windows Server 2003?
12. Поясните назначение смарт-карты.
13. Поясните преимущества аутентификации с помощью смарт-карты.
14. От каких угроз необходимо обеспечивать защиту в корпоративной информационной системе?
15. Для чего предназначен протокол IPSec?
16. Какие средства защиты имеет протокол IPSec ?
17. Для чего предназначено сервер ISA Server 2004 ?
18. Что обеспечивает сервер ISA Server 2004 ?
19. Назовите достоинств сервера ISA Server 2004.
20. Какое назначение имеет Web-сервером Internet Information Services (IIS) ?
21. Для чего предназначены программные продукты семейства Antigen?
22. Назовите преимущества семейства программных продуктов Antigen.
23. Какие виды защиты используются для обеспечения безопасной работы мобильных пользователей?
24. Поясните назначение сервера терминалов (Terminal Server) операционной системы Windows Server 2003.
25. Какие протоколы используются для аутентификации соединений со службами терминалов и шифрования коммуникаций с сервером терминалов ?
26. Какие основные фазы должен реализовывать протокол SSL ?
27. Какие технологии применяются для защиты данных?
28. Поясните сущность технологии кластеризации.
29. Поясните сущность технологии теневого копирования.
30. Для чего предназначен программный продукт Microsoft System Center Data Protection Manager?