Администрирование в информационных системах

Безопасность информационных систем
Шифрование

Информационная безопасность

- Под **информационной безопасностью** понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
- **Защита информации** – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Угрозы информационной безопасности

- **Угроза информационной безопасности** (ИБ) – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
- Попытка реализации угрозы называется **атакой**.
- Классификация угроз ИБ можно выполнить по нескольким критериям:
  - **по аспекту ИБ** (доступность, целостность, конфиденциальность);
  - **по компонентам ИС**, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура);
  - **по способу осуществления** (случайные или преднамеренные действия природного или техногенного характера);
  - **по расположению источника угроз** (внутри или вне рассматриваемой ИС).

Свойства информации

- Вне зависимости от конкретных видов угроз информационная система должна обеспечивать базовые свойства информации и систем ее обработки:
  - **доступность** – возможность получения информации или информационной услуги за приемлемое время;
  - **целостность** – свойство актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения;
  - **конфиденциальность** – защита от несанкционированного доступа к информации.

Примеры реализации угрозы нарушения конфиденциальности

- Часть информации, хранящейся и обрабатываемой в ИС, должна быть сокрыта от посторонних. Передача данной информации может нанести ущерб как организации, так и самой информационной системе.
- Конфиденциальная информация может быть разделена на **предметную** и **служебную**. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, однако ее раскрытие может привести к несанкционированному доступу ко всей информации.
- Предметная информация содержит информацию, раскрытие которой может привести к ущербу (экономическому, моральному) организации или лица.
- Средствами атаки могут служить различные технические средства (подслушивание разговоров, сети), другие способы (несанкционированная передача паролей доступа и т.п.).
- Важный аспект – непрерывность защиты данных на всем жизненном цикле ее хранения и обработки. Пример нарушения – доступное хранение резервных копий данных.

Средства защиты информационных систем

- Такие средства могут быть классифицированы по следующим признакам:
  - **технические средства** – различные электрические, электронные и компьютерные устройства;
  - **физические средства** – реализуются в виде автономных устройств и систем;
  - **программные средства** – программное обеспечение, предназначенное для выполнения функций защиты информации;
  - **криптографические средства** – математические алгоритмы, обеспечивающие преобразования данных для решения задач информационной безопасности;
  - **организационные средства** – совокупность организационно-технических и организационно-правовых мероприятий;
  - **морально-этические средства** – реализуются в виде норм, сложившихся по мере распространения ЭВМ и информационных технологий;
  - **законодательные средства** – совокупность законодательных актов, регламентирующих правила пользования ИС, обработку и передачу информации.

Шифрование

- Одним из способов защиты данных, предоставляемых Интернет-службами, является метод SSL-шифрования и аутентификации на веб-сайтах.
- Используются три вида сертификатов:
  - Сертификаты сервера;
  - Сертификаты клиента;
  - Сертификаты подписывания кода.

Сертификаты сервера

- Сертификаты сервера обеспечивают метод шифрования данных, передаваемых через сеть посредством SSL и методы идентификации сервера.
- Методы позволяют клиенту быть уверенным в подлинности сайта, который он посетил.

Сертификаты клиента.

- Сертификаты клиента обеспечивают идентификацию клиента на сервере, что позволяет серверу определить, кем на самом деле является клиент.
- Данная аутентификация является более предпочтительной по сравнению с базовой.
- Сертификаты клиентов не поддерживают шифрование данных.

Сертификаты подписания кода

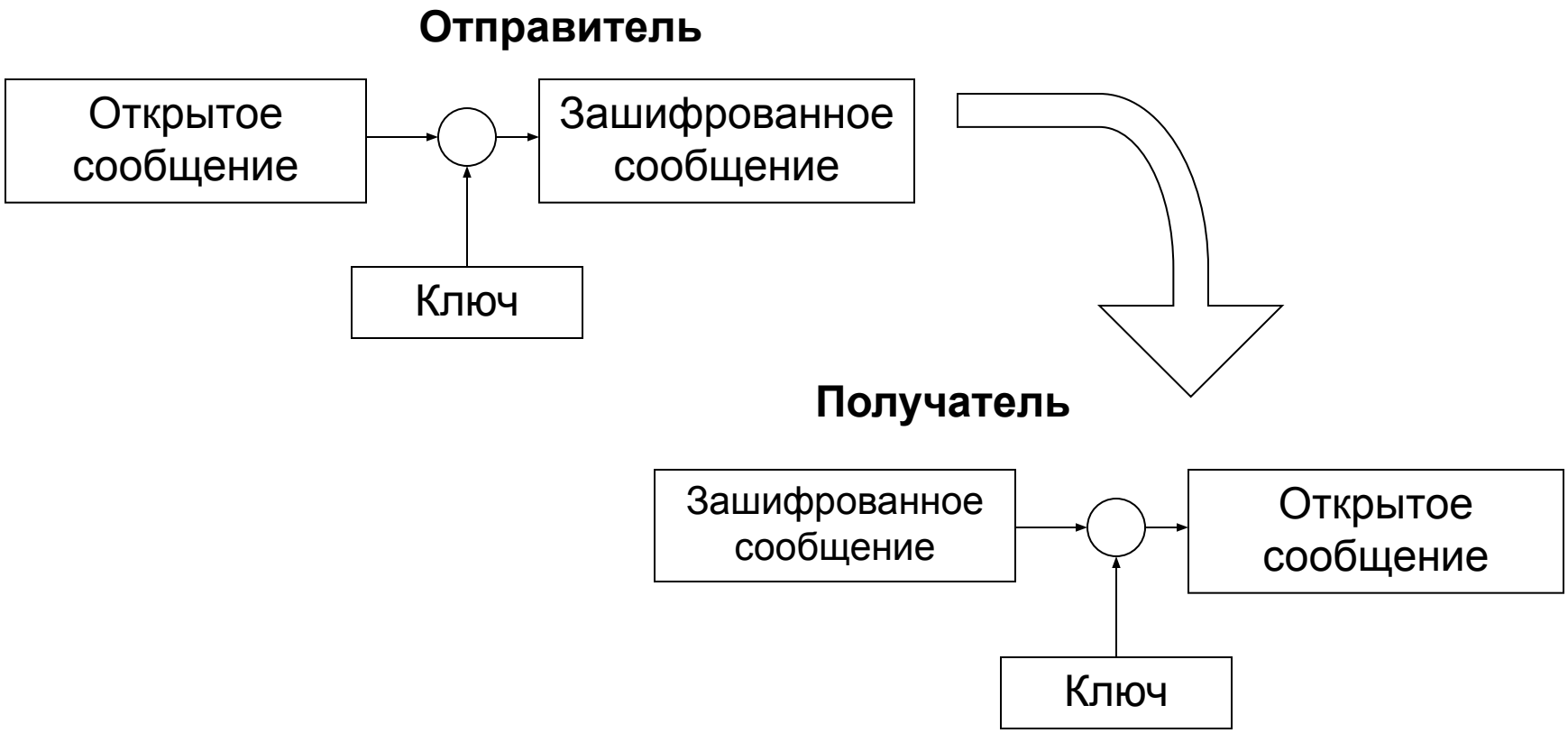
- Сертификаты подписывания кода обеспечивают метод шифрового «подписывания» приложения посредством цифрового идентификатора, созданного на основе содержимого приложения.
- Если в приложении произошли изменения, то цифровой идентификатор теряет соответствие этому приложению и пользователь получает уведомление.
- Сертификаты подписывания не поддерживают шифрования приложений.

Ключи сертификатов

- Цифровые сертификаты используют ключи при шифровании данных.
  - **Ключ** – фрагмент данных, используемых криптографической системой для преобразования открытого текста в шифрованный текст.
- **Криптографическое преобразование** (шифрование) – это математический алгоритм преобразования цифровых данных.

Криптографические средства защиты данных

- Для обеспечения защиты информации в распределенных информационных системах активно применяются криптографические средства защиты информации.
- Сущность криптографических методов заключается в следующем:



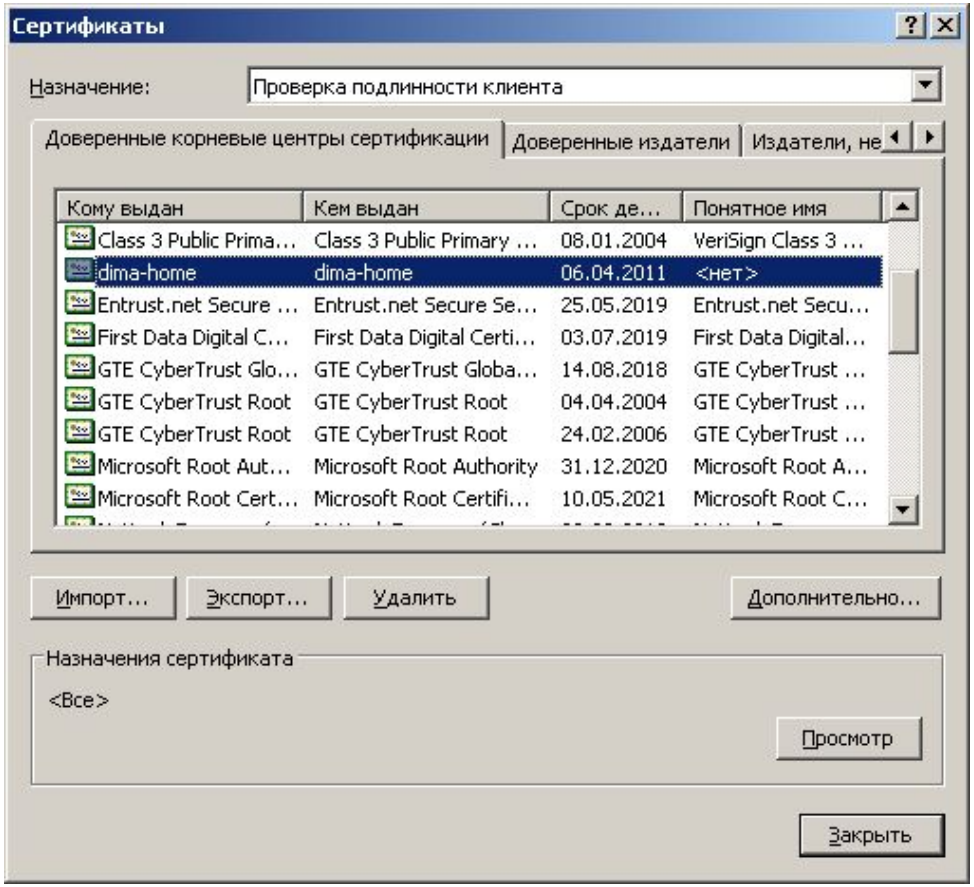
Бюро сертификатов и доверие

- При создании пары ключей (в алгоритмах несимметричного шифрования) для использования на веб-сайте, запрашивается сертификат SSL X.509 у **бюро сертификатов** – сервера, выпускающего сертификаты.
- Бюро сертификатов может организовывать иерархическую структуру - авторизовать (уполномочить) любое число сертификатов, те, в свою очередь, другие бюро и т.д.
- Первое бюро сертификатов называется **корневым**.

Использование бюро сертификатов на компьютере клиента

- На клиенте может быть установлен набор сертификатов по умолчанию, выпустившие их бюро сертификатов являются доверенными.
- При представлении клиенту сертификата SSL клиент выяснит, имеется ли в его кэше соответствующий сертификат.
- При наличие сертификата клиент проверяет подпись бюро сертификатов при помощи открытого ключа, находящегося в кэше, осуществив аутентификацию сервера.
- Если сертификат отсутствует в кэше, клиент запросит сертификат и повторит проверку сертификата.

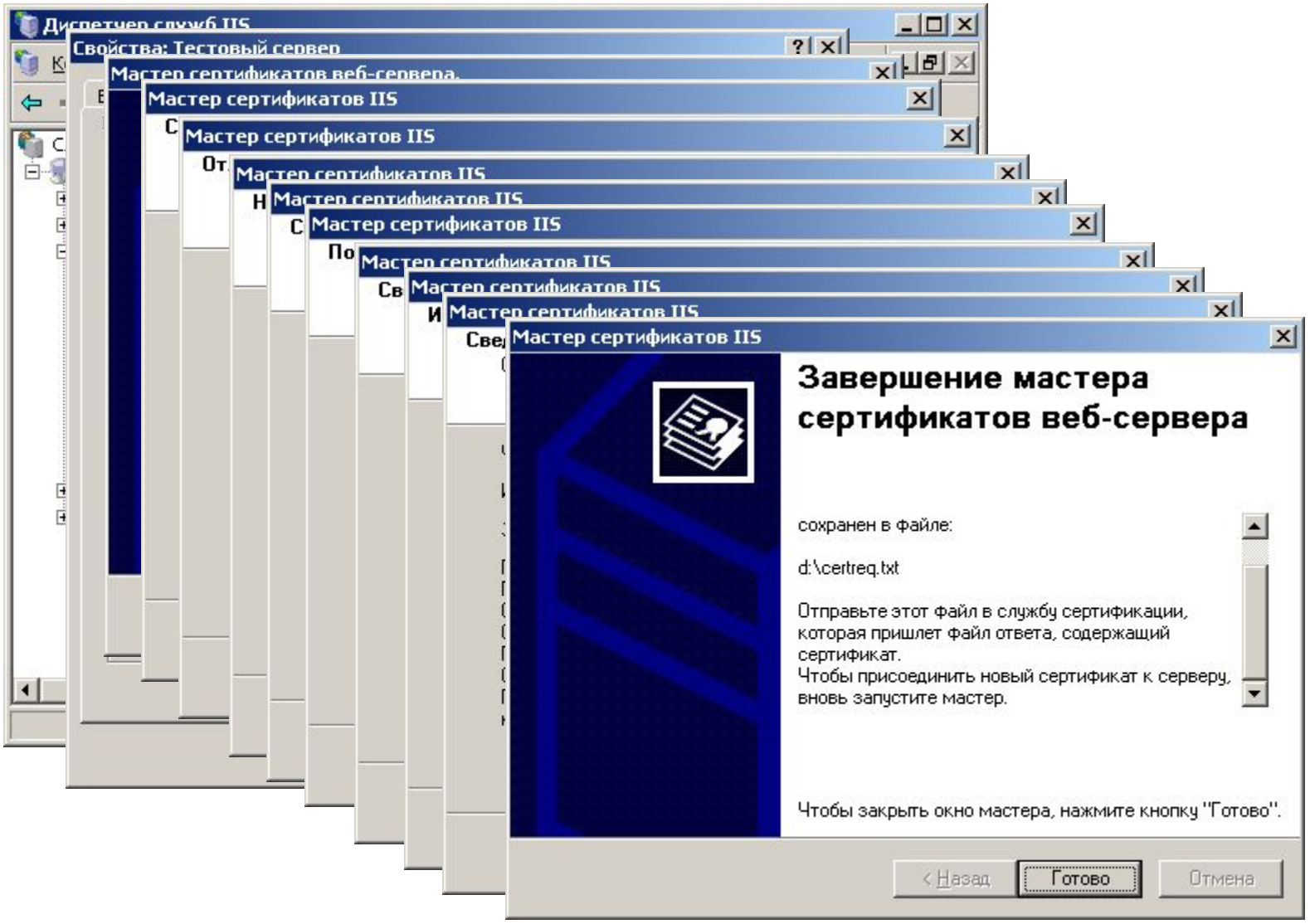
Список доверенных бюро сертификатов



Создание собственного бюро сертификатов

- Для установки собственного бюро сертификатов необходима установка **служб сертификатов** на сервер.
- Установка выполняется стандартным образом с помощью мастера установки и удаления программ.
- Установка различается для разных типов бюро:
  - Корпоративное корневое бюро сертификатов
  - Корпоративное подчиненное бюро сертификатов
  - Отдельное корневое бюро сертификатов
  - Подчиненное бюро сертификатов.

Создание запроса на сертификат в IIS

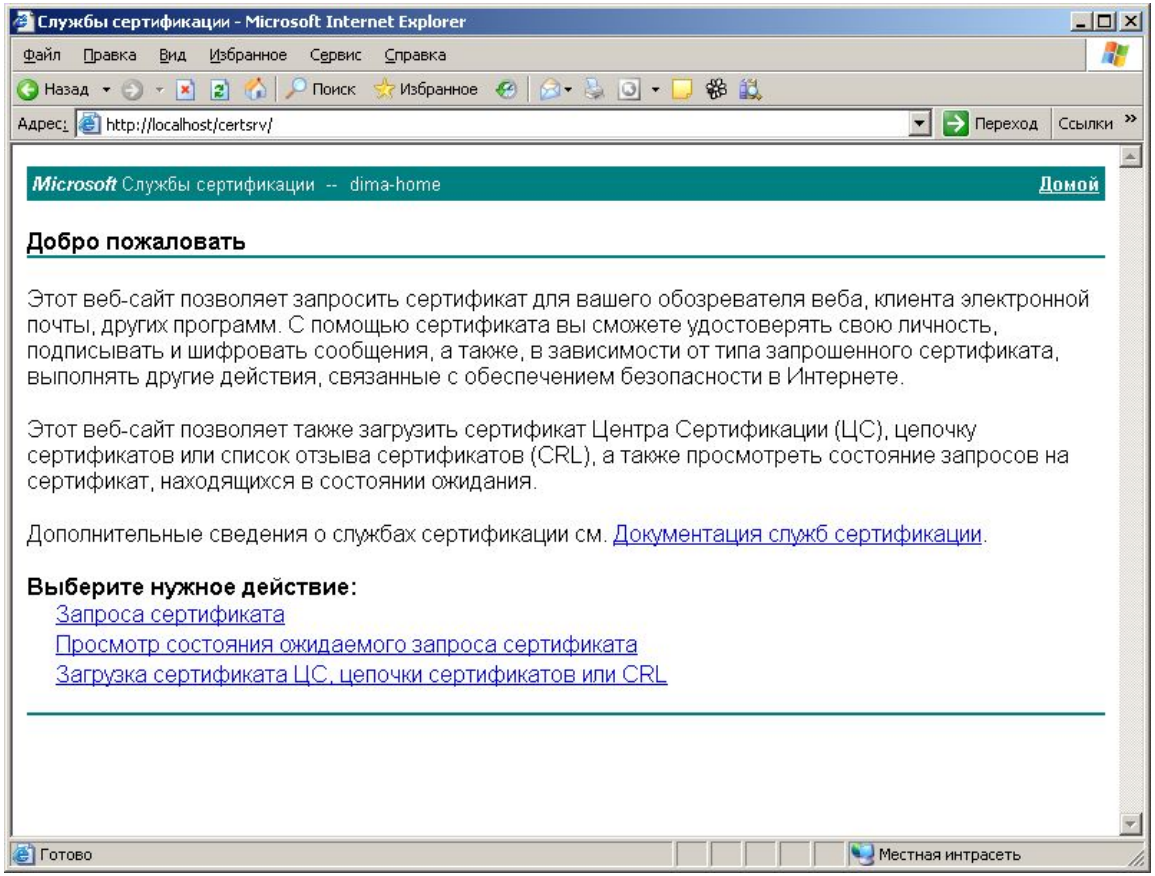


Отправка запроса в собственное бюро

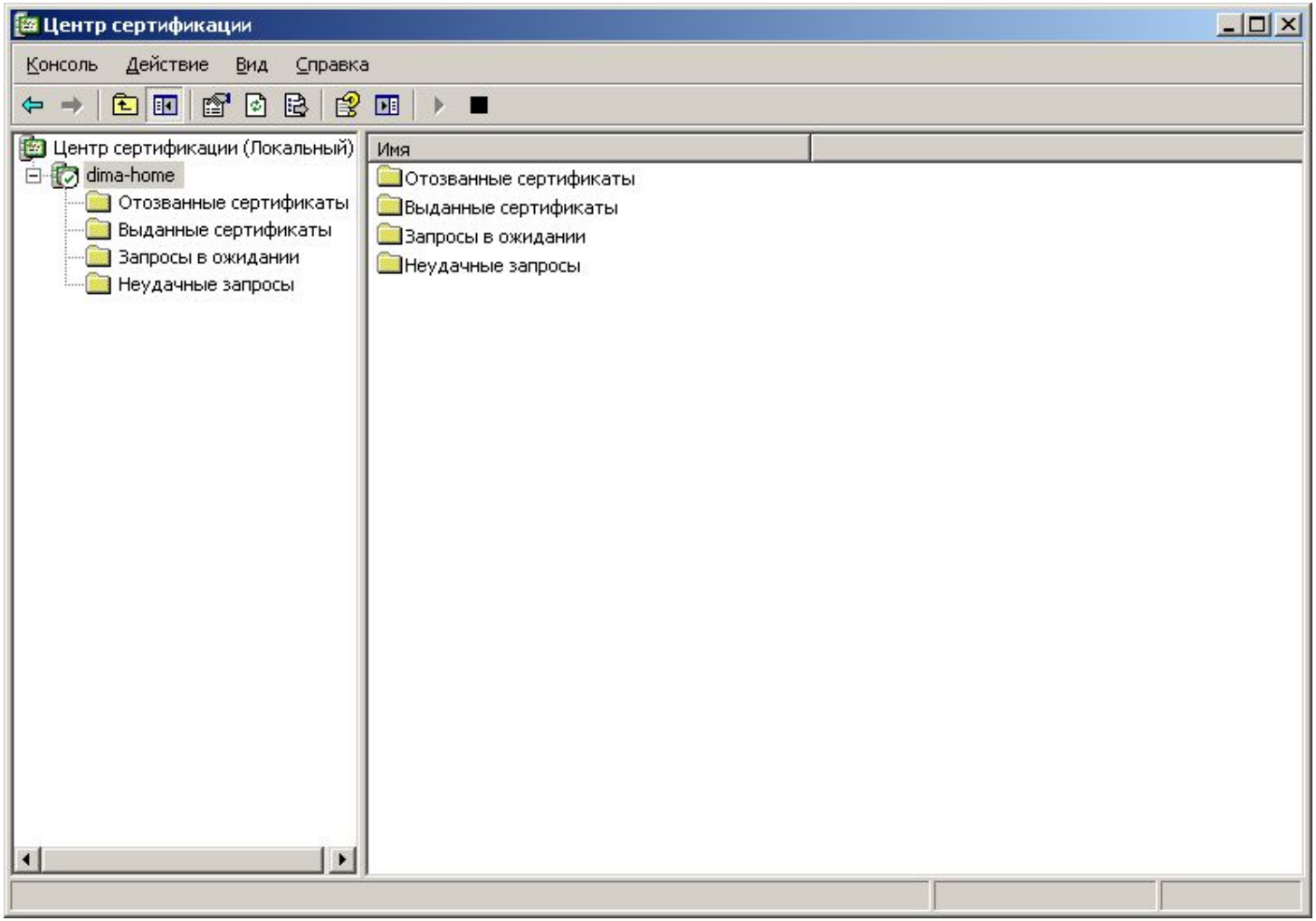
- Для запроса сертификата у собственного бюро сертификации можно двумя способами:
  - С помощью Интернет регистрации;
  - Отправка запроса через оснастку **Сертификаты**.

Использование Интернет регистрации

- Для доступа к интернет-регистрации бюро сертификатов выполняется через страницу http://<ваш_сервер>/crtsrv.



Отправка запроса из оснастки Центр сертификатов



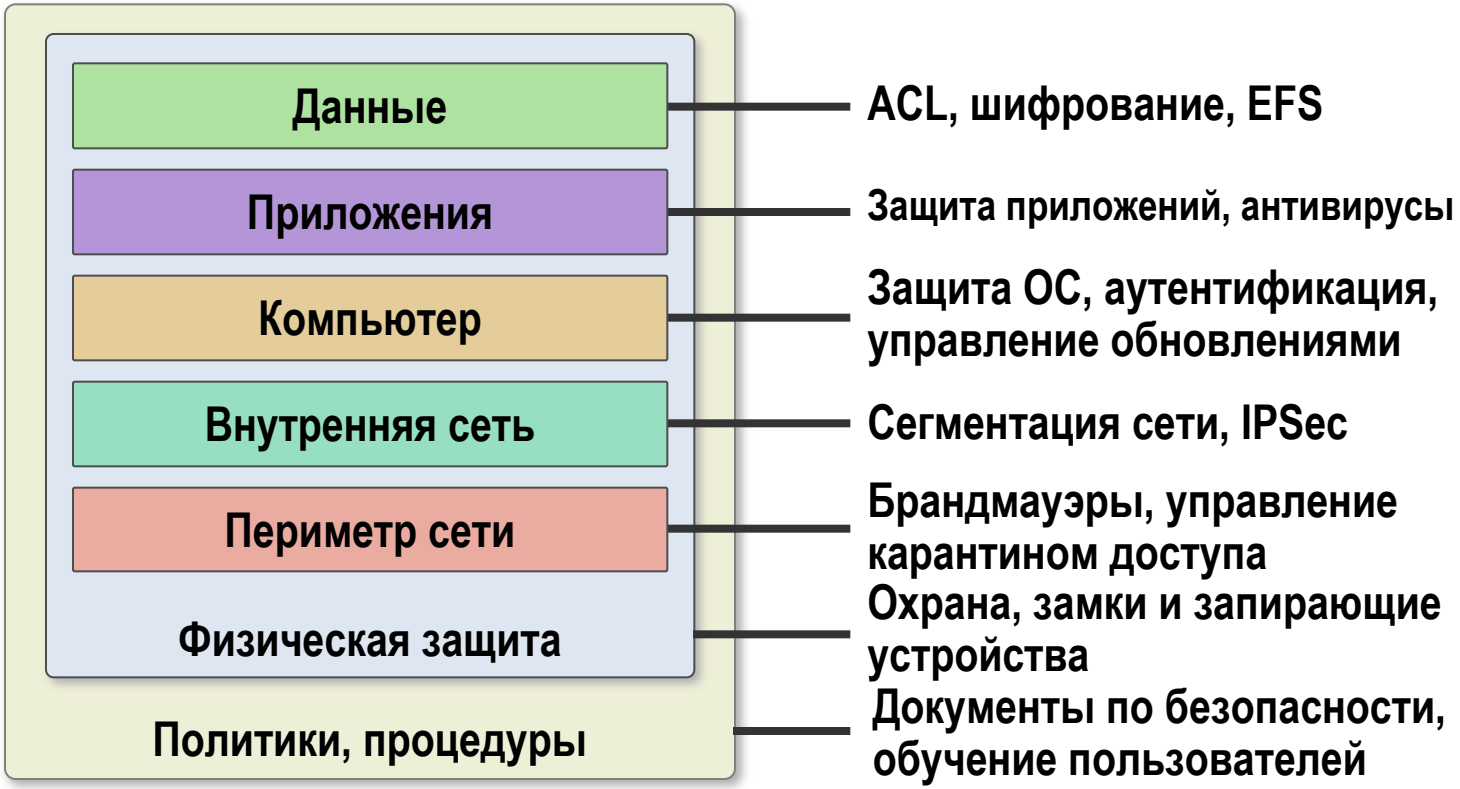
Защита данных в информационных системах

- Для обеспечения защиты данных в информационных системах проводится анализ угроз информационной безопасности, строится модель действий нарушителя и вырабатываются меры по противодействию.
- Для упрощения анализа и выработки мер строится многослойная модель защиты.

Модель многослойной защиты

Использование многослойной модели защиты позволяет:

- **Уменьшить шанс успеха атаки**
- **Увеличить вероятность обнаружения атаки**



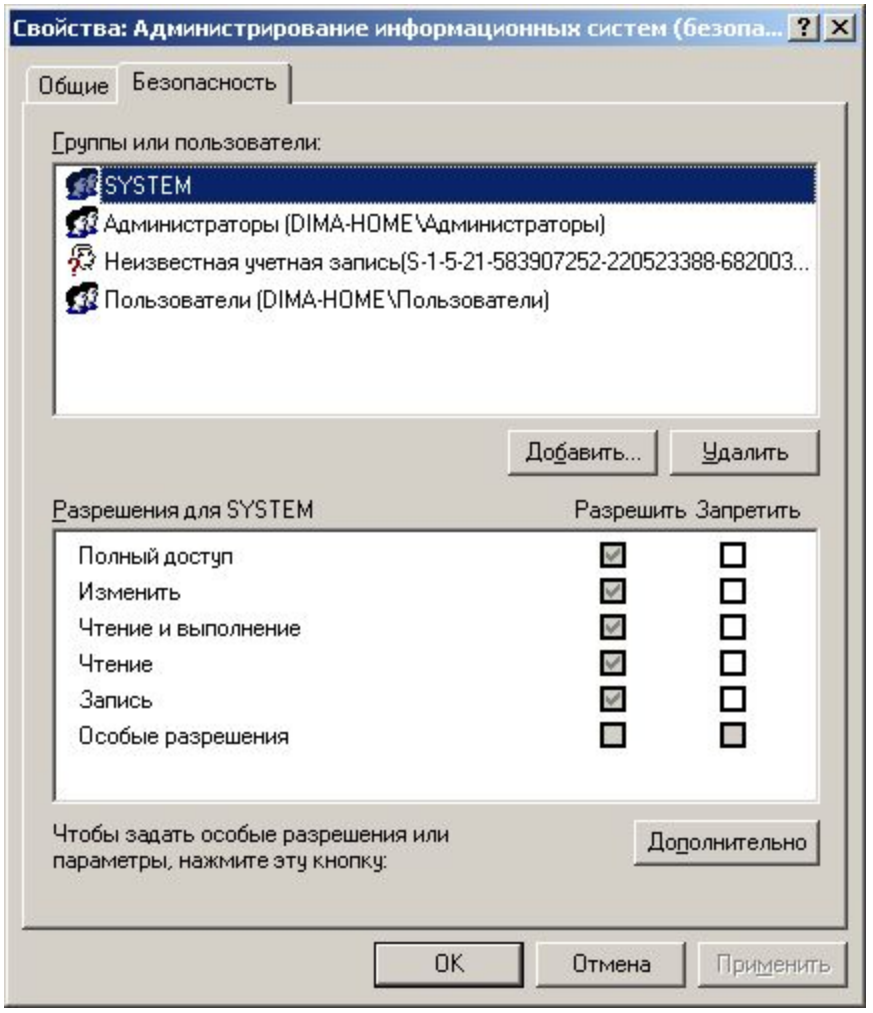
Модель многослойной защиты

Управление доступом

- Одним из средств защиты данных является **механизм управления доступом**.
  - Управление доступом на уровне данных в ОС Windows 2000/XP/2003 эффективно выполняется на носителях с файловой системой NTFS.
  - Файловая система NTFS обеспечивает поддержку хранения списков прав доступа (ACL) и механизм их использования при выдаче разрешений и запретов на операции с файлами и каталогами.

Управление доступом

- Управление доступом к локальным папкам и каталогам на разделах NTFS выполняется с помощью специальной закладки **Безопасность** в окне **Свойство** папки или каталога.
- Управляющие кнопки **Добавить** и **Удалить** обеспечивают управление пользователями, нижнее окно позволяет устанавливать разрешения для выбранного объекта.
- Поддерживается групповое управление.



Управление доступом

- Для управления разрешениями в режиме командной строки используется команда **cacls**.
- **Синтаксис данной команды**:
  - **cacls** *имя_файла* [**/t**] [**/e** [**/r** *пользователь* [...]]] [**/c**] [**/g** *пользователь*:*разрешение*] [**/p** *пользователь*:*разрешение* [...]] [**/d** *пользователь* [...]]
- **Ключи команды**:
  - **/t** - Изменение таблиц контроля доступа (DACL) указанных файлов в текущем каталоге и всех подкаталогах
  - **/e** - Редактирование таблицы управления доступом (DACL) вместо ее замены
  - **/r** *пользователь* - Отмена прав доступа для указанного пользователя. Недопустим без параметра **/e**
  - **/c** - Продолжение внесения изменений в таблицы управления доступом (DACL) с игнорированием ошибок
  - **/g** *пользователь*:*разрешение* – Предоставление прав доступа указанному пользователю
  - **/p** *пользователь*:*разрешение* - Смена прав доступа для указанного пользователя
  - **/d** *пользователь* - Запрещение доступа для указанного пользователя

Шифрование данных

- Шифрованная файловая система (Encrypting File System, EFS) позволяет безопасно хранить данные. EFS делает это возможным благодаря шифрованию данных в выбранных файлах и папках файловой системы NTFS.
- Файлы и папки на томах с файловой системой FAT не могут быть зашифрованы или расшифрованы.
- EFS разработана для безопасного хранения данных на локальных компьютерах. Поэтому она не поддерживает безопасную передачу файлов по сети.

Ключи шифрования

- *Шифрование* файлов происходит следующим образом:
  - Каждый файл имеет уникальный *ключ шифрования файла*, который позже используется для расшифровки данных файла.
  - Ключ шифрования файла сам по себе зашифрован — он защищен **открытым ключом** пользователя, соответствующим сертификату EFS.
  - Ключ шифрования файла также защищен открытым ключом каждого дополнительного пользователя EFS, уполномоченного расшифровывать файлы, и ключом каждого **агента восстановления**.
- Сертификат и закрытый ключ системы EFS могут быть выданы несколькими источниками. Сюда входит автоматическое создание сертификатов и выдача сертификатов центрами сертификации (ЦС) корпорации Майкрософт или сторонними центрами сертификации

Расшифровывание данных

- *Расшифровка* файлов происходит следующим образом:
  - Для расшифровки файла необходимо сначала расшифровать его ключ шифрования. Ключ шифрования файла расшифровывается, если **закрытый ключ** пользователя совпадает с открытым.
  - Не только пользователь может расшифровать ключ шифрования файла. Другие назначенные пользователи или агенты восстановления также могут расшифровать ключ шифрования файла, используя собственный закрытый ключ.
- Закрытые ключи содержатся в защищенном хранилище ключей, а не в диспетчере учетных записей безопасности (Security Account Manager, SAM) или в отдельном каталоге.

Хранение зашифрованных данных на удаленных серверах

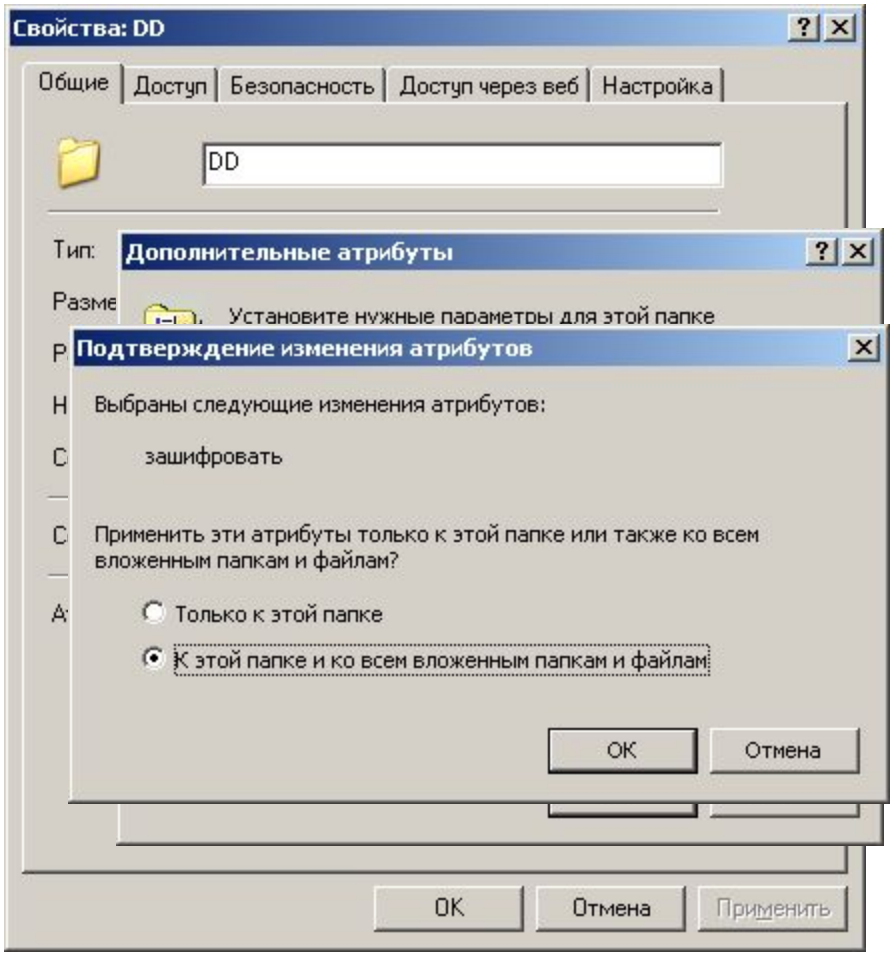
- Если пользователям рабочей среды семейства Windows Server 2003 или Windows XP нужно хранить зашифрованные файлы на удаленных серверах, необходимо помнить.
  - В семействе Windows Server 2003 и Windows XP поддерживается хранение зашифрованных файлов на удаленных серверах.
  - Пользователи могут удаленно применять шифрованную файловую систему только тогда, когда оба компьютера являются членами одного леса семейства Windows Server 2003.
  - Зашифрованные данные не шифруются при передаче по сети, а только при сохранении на диске. Исключения составляют случаи, когда система включает протокол IPSec или протокол WebDAV. IPSec шифрует данные при передаче по сети TCP/IP. Если файл был зашифрован перед копированием или перемещением в папку WebDAV на сервере, он останется зашифрованным при передаче и во время хранения на сервере.
  - Не поддерживается хранение сертификатов и закрытых ключей шифрованной файловой системы на смарт-картах.
  - Не поддерживается усиленная защита закрытых ключей для закрытых ключей EFS.

Управление сертификатами

- Шифрованная файловая система (EFS) с помощью криптографии открытого ключа шифрует содержимое файлов. В ней применяются ключи, полученные от сертификата пользователя и дополнительных пользователей, а также от назначенных агентов восстановления шифрованных данных, которые настроены.
- Сертификаты, используемые файловой системой EFS, могут быть получены в центре сертификации (ЦС) или же автоматически созданы компьютером. При получении EFS сертификата в центре сертификации необходима ссылка сертификата на поставщика службы криптографии (CSP) и соответствующий идентификатор объекта (OID). В EFS возможно использование основного или расширенного CSP.
  - Сертификаты и закрытые ключи от всех назначенных агентов восстановления шифрованных данных необходимо экспортировать на съемный диск или хранить в безопасности до тех пор, пока они не понадобятся.

Шифрование файлов

- Для выполнения шифрования данных можно воспользоваться кнопкой **Другие** в закладке **Свойства** файла.
- Для удобства пользователя зашифрованные папки и файлы отображаются другим цветом.



Использование утилит командной строки

- Для просмотра информации о зашифрованных файлах можно воспользоваться утилитой **efsinfo**
  - Синтаксис команды
    - **efsinfo**[**/u**] [**/r**] [**/c**] [**/i**] [**/y**] [**/k**] [**/s:каталог**] [*Путь*[, *Путь*...]][**/?**]
    - **efsinfo /t:** *каталог*

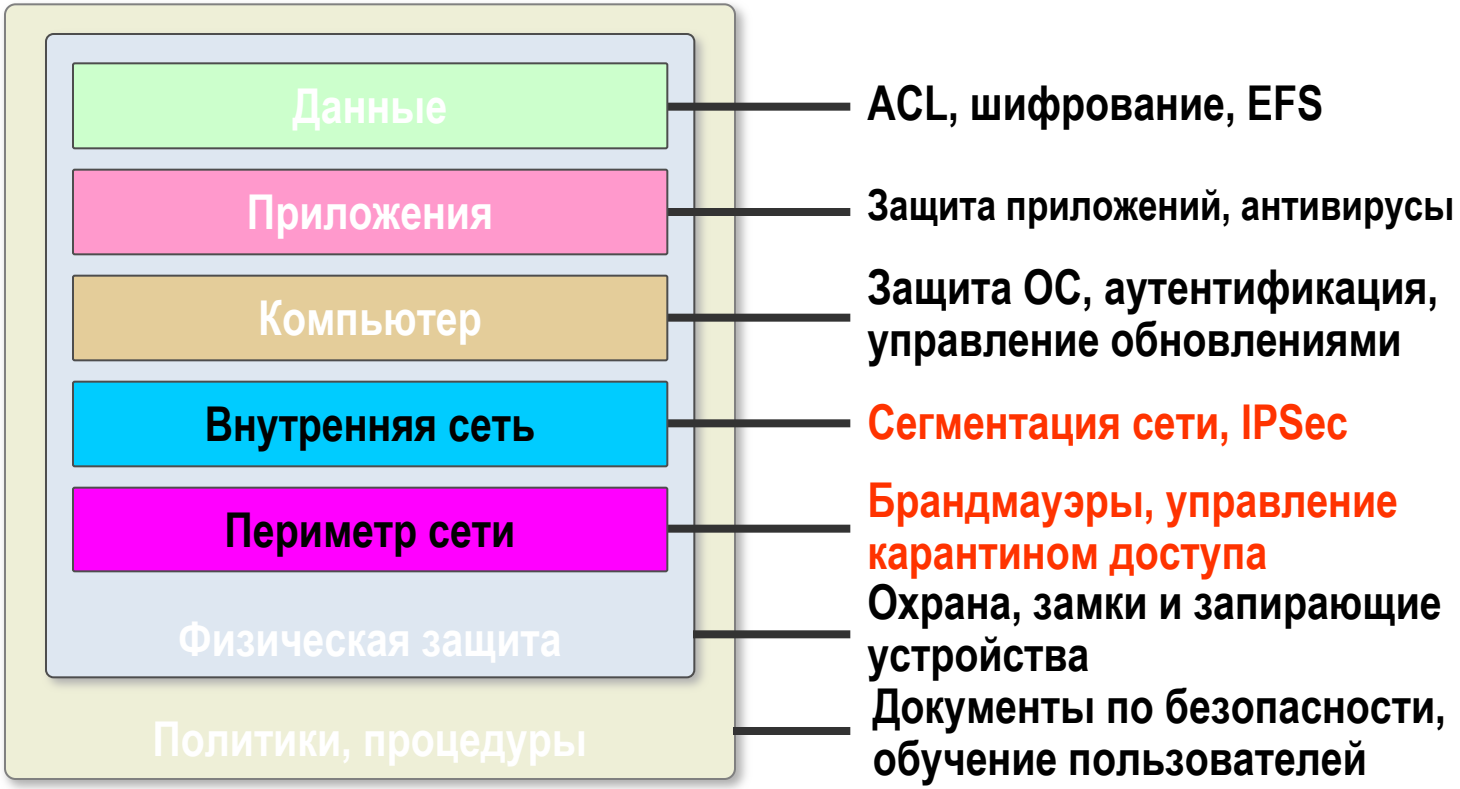
Использование утилит командной строки

- Отображение или изменение шифрование папок и файлов на томах NTFS.
- Использованная без параметров команда **cipher** отображает состояние шифрования текущей папки и всех файлов, находящихся в ней.
  - **Синтаксис команды**
    - **cipher** [{**/e** | **/d**}] [**/s:***папка*] [**/a**] [**/i**] [**/f**] [**/q**] [**/h**] [**/k**] [**/u**[**/n**]]
      [{*путь* [...]] | **/r:***имя_файла_без_расширения* | **/w:***путь* | **/x**[**:***путь*] *имя_файла_без_расширения*}]

Цели обеспечения безопасности сети

	Защита периметра	Защита клиентов	Обнаружение вторжений	Контроль доступа к сети	Конфиден-циальность	Безопасность удаленного доступа
ISA Server	✔		✔	✔		✔
Windows Firewall		✔				
IPSec		✔			✔	✔
Network Access Quarantine				✔		✔

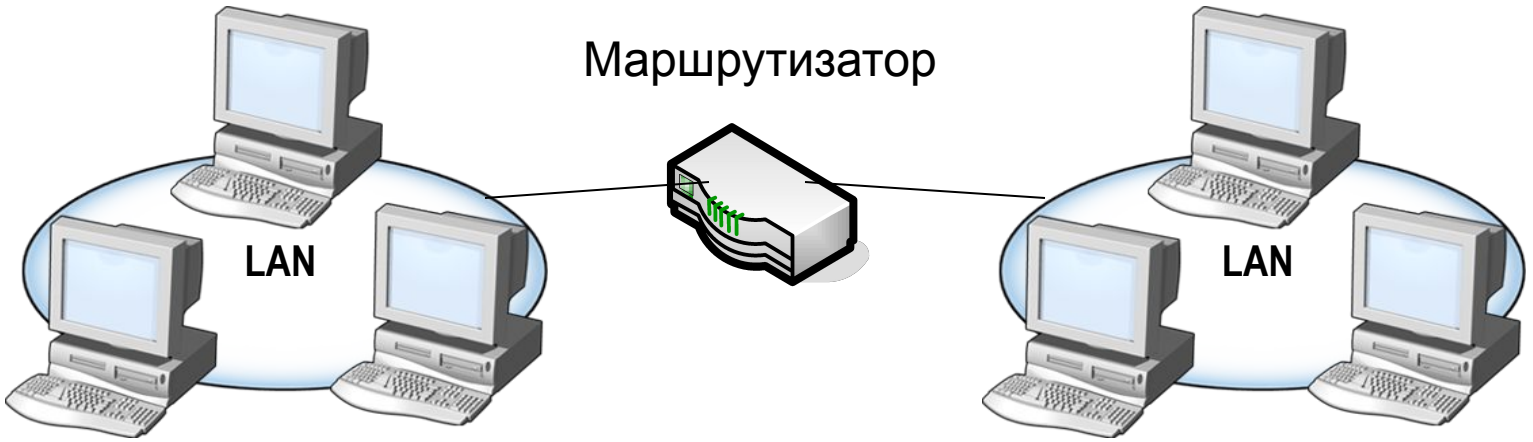
Модель многослойной защиты



Сегментация сети

- Одним из средств защиты передачи данных является механизм сегментации сети (деление на подсети).
- Механизм разделения общей сети на отдельные подсети предприятия позволяет скрывать детали отдельных подсетей, обеспечивает возможность контроля трафика на границе подсети.

Сегментация сети



Отдельные сегменты сети

Сегментация сети средствами Windows

- Для обеспечения разделения внутренней сети организации на отдельные сегменты возможно использование аппаратных (коммутаторы) и программно-аппаратных (маршрутизаторы) решений.
  - Серверная платформа Windows 2000/2003 позволяет создание эффективного маршрутизатора с возможностями усиления безопасности на границах сетей. Инструментом является служба **Удаленный доступ и маршрутизация (RRAS)**.

Служба Маршрутизация и удаленный доступ

- Служба **Маршрутизация и удаленный доступ** (Routing and Remote Access, RRAS) в Windows 2003 – программный многопротокольный маршрутизатор, который может быть объединен с другими функциями ОС, такими как управление безопасностью на основе учетных записей и групповых политик.
  - Служба поддерживает маршрутизацию между различными ЛВС, между ЛВС и WAN-каналами, VPN- и NAT- маршрутизацию в IP-сетях.

Особенности Службы маршрутизации и удаленного доступа

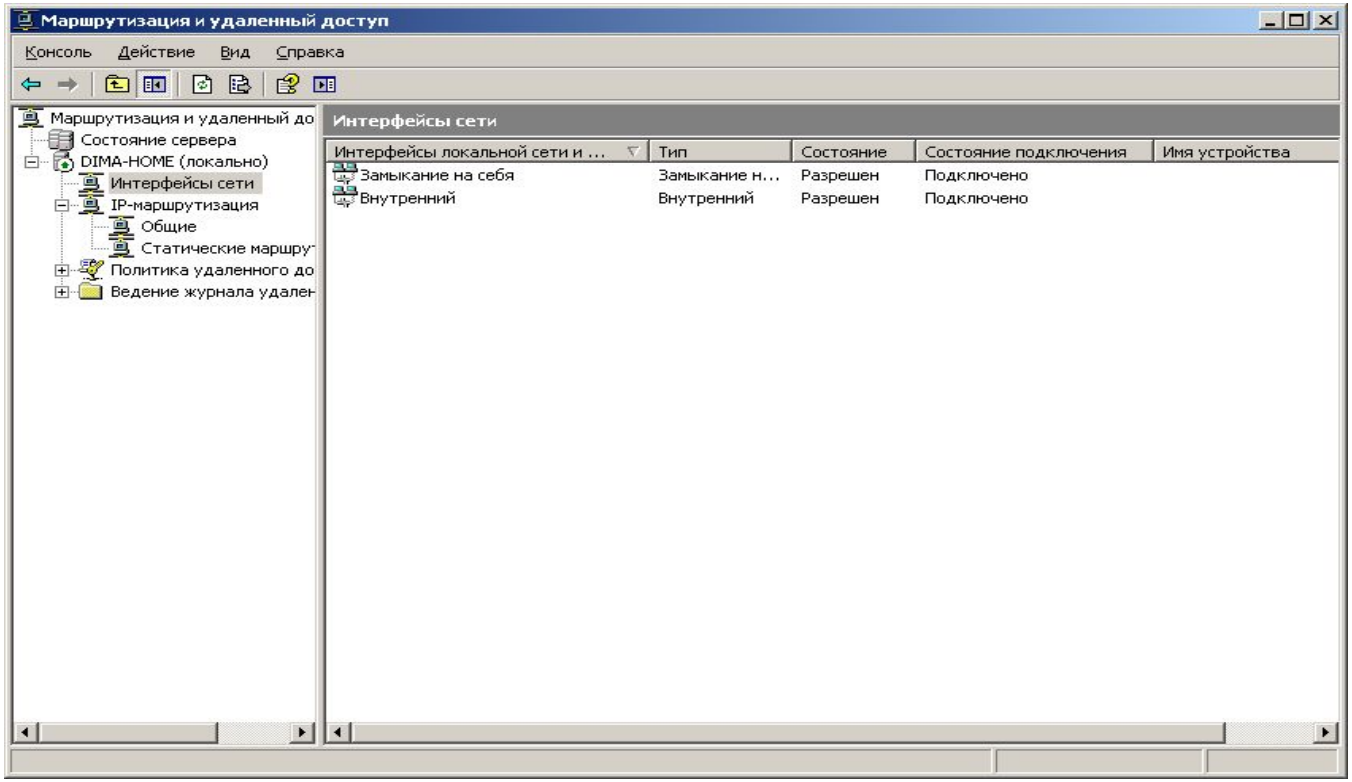
- Кроме того, служба может быть сконфигурирована для особого вида маршрутизации:
  - Многоадресные ip-рассылки;
  - Маршрутизация вызовов по требованию;
  - Ретрансляция DHCP;
  - Фильтрация пакетов
- В службу включена поддержка протоколов **динамической маршрутизации** – RIP (routing information protocol) и OSPF (open shortest path first).

Запуск службы Маршрутизация и удаленный доступ

- При установки Windows server 2003 служба Маршрутизация и удаленный доступ отключена.
- Ее активация выполняется с помощью Мастера настройки сервера маршрутизации и удаленного доступа.
- Если сервер маршрутизации является рядовым членом домена Active Directory, то он должен быть включен в группу Серверы RAS и IAS.
- Контроллеры домена в дополнительной настройке не нуждаются.

Консоль управления Маршрутизация и удаленный доступ

- Консоль управления Маршрутизация и удаленный доступ представляет собой стандартную оснастку консоли управления в Windows. В конфигурации по умолчанию поддерживается маршрутизация в ЛВС.

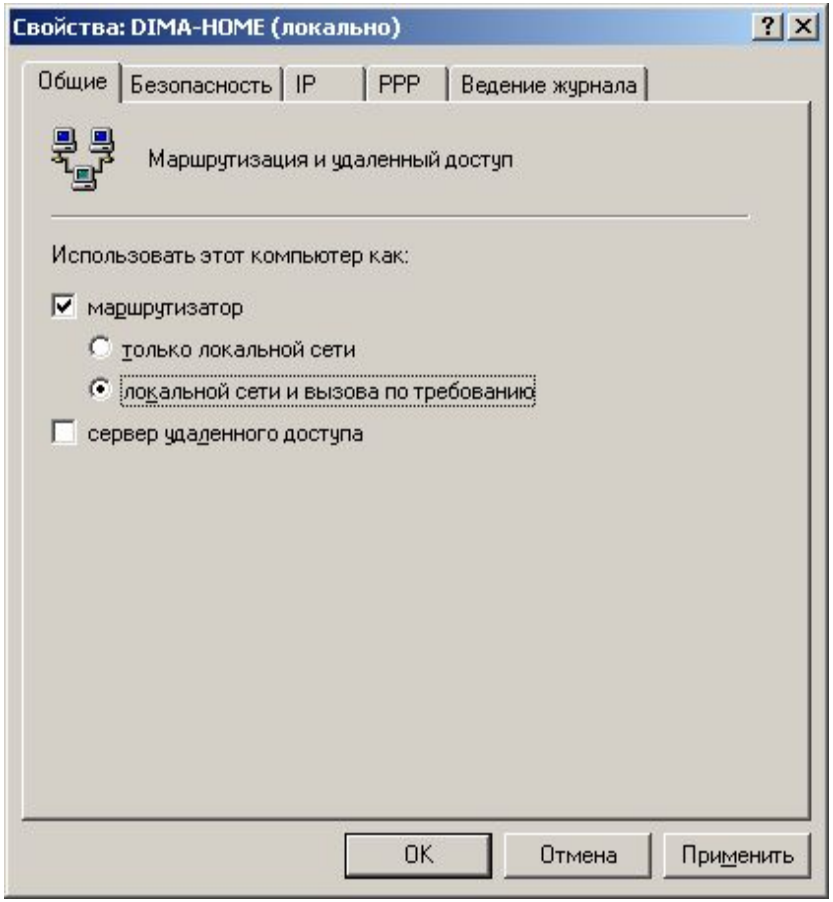


Создание сетевых интерфейсов

- Сетевой интерфейс в консоли управления – программный компонент, подключаемый к физическому устройству (модему или сетевой плате).
  - Все интерфейсы, через которые необходимо маршрутизировать трафик должны присутствовать в консоли управления.
- Если необходимо сконфигурировать маршрутизацию через подключение по требованию или постоянное подключение по коммутируемой линии, VPN или PPOE-подключение (Point-to-Point Protocol over Ethernet), необходимо выполнить конфигурирование интерфейсов в ручную.

Создание интерфейсов по вызову

- Для создания интерфейса по вызову, необходимо включить такую возможность в **Свойствах** сервера маршрутизации.
- Для создания подключения используется Мастер интерфейса по требованию

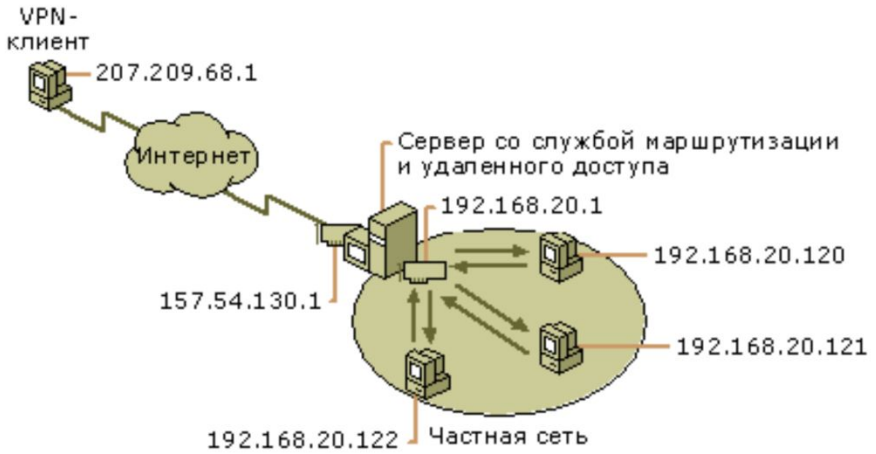


Удаленный доступ (модем)

- При выборе данного пути сервер со службой маршрутизации и удаленного доступа настроен для разрешения подключения клиентов удаленного доступа к частной сети с помощью вызова банка модема или другого оборудования удаленного доступа.
- Дополнительные настройки:
  - установка ответа сервера на вызов;
  - установка разрешений для клиентов удаленного доступа для подключения к частной сети и перенаправления сетевого трафика между клиентами удаленного доступа и частной сетью.

Удаленный доступ (VPN)

- При выборе данного пути сервер со службой маршрутизации и удаленного доступа настроен для разрешения подключения клиентов удаленного доступа к частной сети через Интернет.
- После окончания работы мастера можно настроить дополнительные параметры.
  - Например, можно настроить: как сервер проверяет разрешения клиентов VPN для подключения к частной сети и направляет ли сервер сетевой трафик между клиентами VPN и частной сетью.



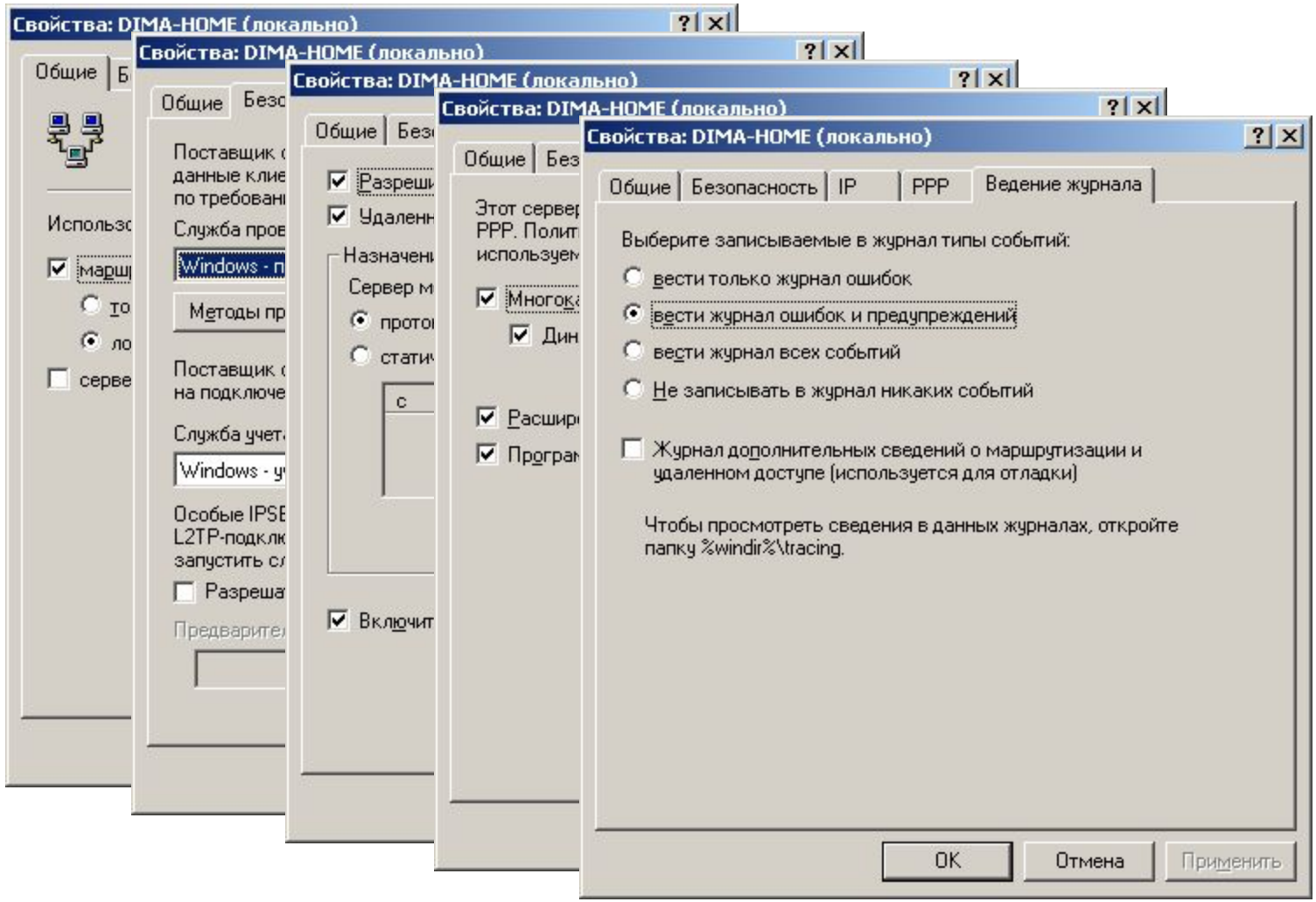
Преобразование сетевых адресов (NAT)

- При выборе данного пути сервер со службой маршрутизации и удаленного доступа настроен для совместного использования с компьютерами частной сети подключения к Интернету и для передачи трафика между общим адресом и частной сетью.
- После окончания работы мастера можно настроить дополнительные параметры.
  - Например, можно настроить фильтры пакетов и выбрать службы для общего интерфейса.

IP - маршрутизация

- Узел ip – маршрутизация используется дла настройки основных параметров по протоколу IP.
- По умолчанию содержится три подузла:
  - Общие
  - Статические маршруты
  - NAT / простой брандмауэр

Настройка параметров службы маршрутизации и удаленного доступа



Управление таблицей маршрутизации

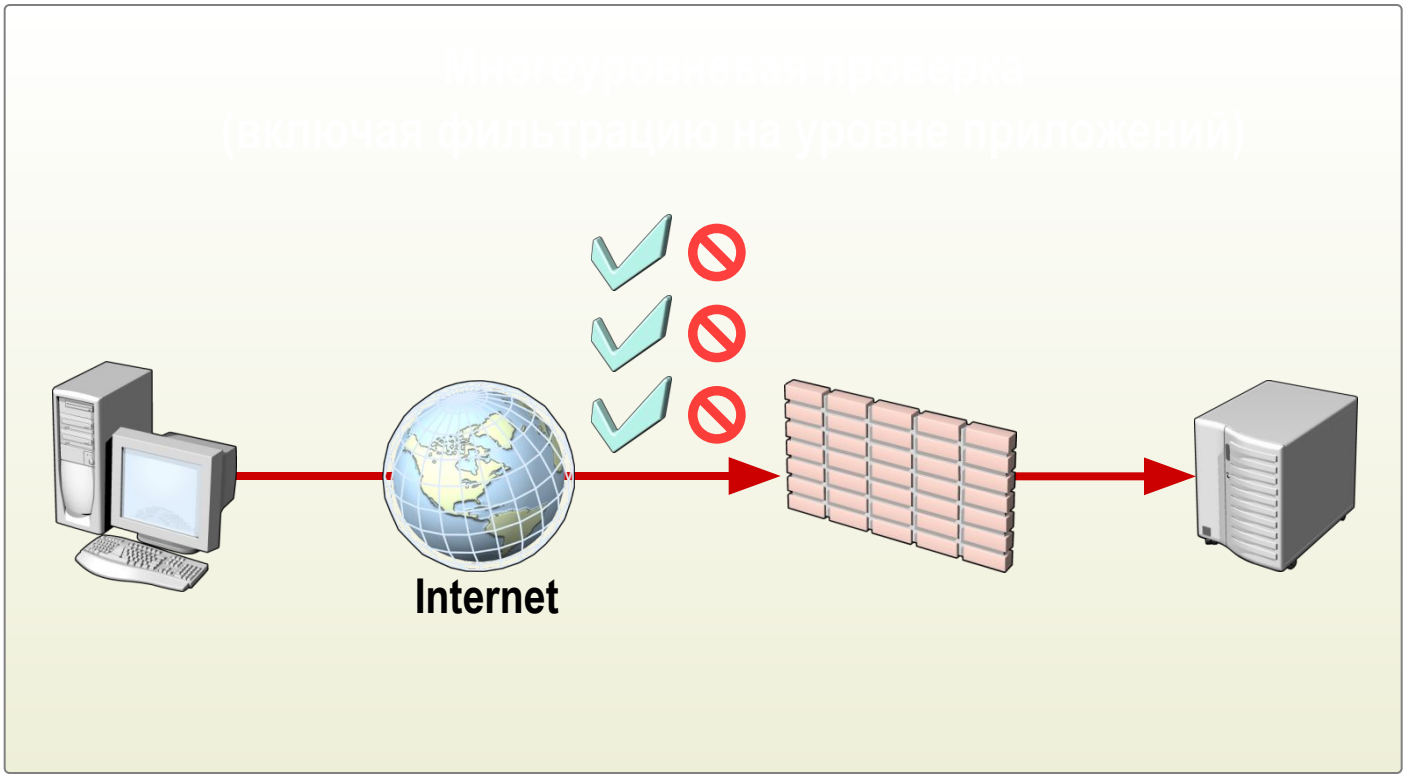
- Мрашрутизаторы считывают адреса назначения пакетов и переправляют пакеты в соответствии с информацией, хранящейся в таблицах маршрутизации.
- Отдельные записи таблицы маршрутизации называются маршрутами.
- Существуют три типа маршрута:
  - Маршрут узла – определяет ссылку на определенный узел или широковещательный адрес. Маска маршрута – 255.255.255.255;
  - Маршрут сети – определяет маршрут к определенной сети, а соответствующее поле в таблицах маршрутизации может содержать произвольную маску;
  - Маршрут по умолчанию – один маршрут, по которому отправляются все пакеты, чей адрес не совпадает ни с одним адресов таблицы маршрутизации.
- Просмотр таблицы маршрутизации может быть выполнен с помощью команд
  - **route print**
  - **netstat -r**

Защита периметра сети

- **Защита периметра сети** предусматривает создание условий препятствующих проникновению постороннего трафика из внешней сети во внутреннюю сеть организации (и возможно ограничение трафика из внутренней сети во внешнюю).
  - Одним из средств защиты является использование **брандмауэров (межсетевых экранов)**.

Функции сетевых брандмауэров

- Фильтрация пакетов
- Проверка установки соединений
- Проверка трафика на уровне приложений



Защита клиентов

Метод	Описание
Прокси-функции	**Обработка всех запросов клиентов и запрет прямых соединений**
Поддержка клиентов	**Возможность поддержки подключений клиентов без специального ПО. Использование специального ПО (ISA Firewall) обеспечивает дополнительную функциональность**
Правила	**Доступ к веб-ресурсам может быть ограничен на основе имени пользователя, IP-адреса клиента, URL сервера или по расписанию**
Add-ons	**Дополнительные компоненты обеспечвают расширение функциональности брандмауэра и возможность использования решений третих фирм**

Защита веб-серверов

- Правила веб-публикаций
  - Защита веб-серверов, находящихся позади брандмауэра предотвращает внешние атаки на сервера путем проверки HTTP входящего трафика
- Проверка Secure Socket Layer (SSL) трафика
  - Расшифровка и проверка входящего зашифрованного веб-трафика на предмет соответствия заданным правилам и стандартам
  - Возможна перешифровка трафика перед пересылкой на веб-сервер

HTTP фильтрация

- Интернет приложения используют HTTP для туннелирования трафика приложений
- ISA Server 2004 включает HTTP фильтры для:
  - Обеспечения контроля за всем HTTP трафиком
  - Обеспечения URLScan функциональности по периметру сети организации
  - Возможность объединения с URLScan внутренних веб-серверов для обеспечения согласования разрешенного трафика
- HTTP фильтры могут обеспечить фильтрацию:
  - На основе анализа HTTP запросов, ответов, заголовков и содержания контента
  - На основе расширений файлов, методов передачи и цифровых подписей