

# Средства защиты в почтовом сервере Exchange 2003

*Шаститко Игорь*  
*Microsoft Certified Trainer*

# Задачи по обеспечению безопасности Exchange 2003

- Защита сервера Exchange от внешних угроз
- Защита почтовых ящиков пользователей от нежелательной почты и вирусов
- Обеспечение безопасной работы клиентов и передачи данных, аутентификация при работе со службами Exchange
- Обеспечение безопасного администрирования серверов Exchange
- Обеспечение высокой доступности служб Exchange

# Защита от внешних угроз

- Требующие внимания угрозы
  - Уязвимости кода операционной системы, сервера Exchange и отдельных служб
  - Уязвимости, связанные с неверной конфигурацией сервера Exchange
  - Атаки на порты операционной системы и сервера
  - Атаки на отказ в обслуживании, связанные с различными службами Exchange

# Защита от внешних угроз

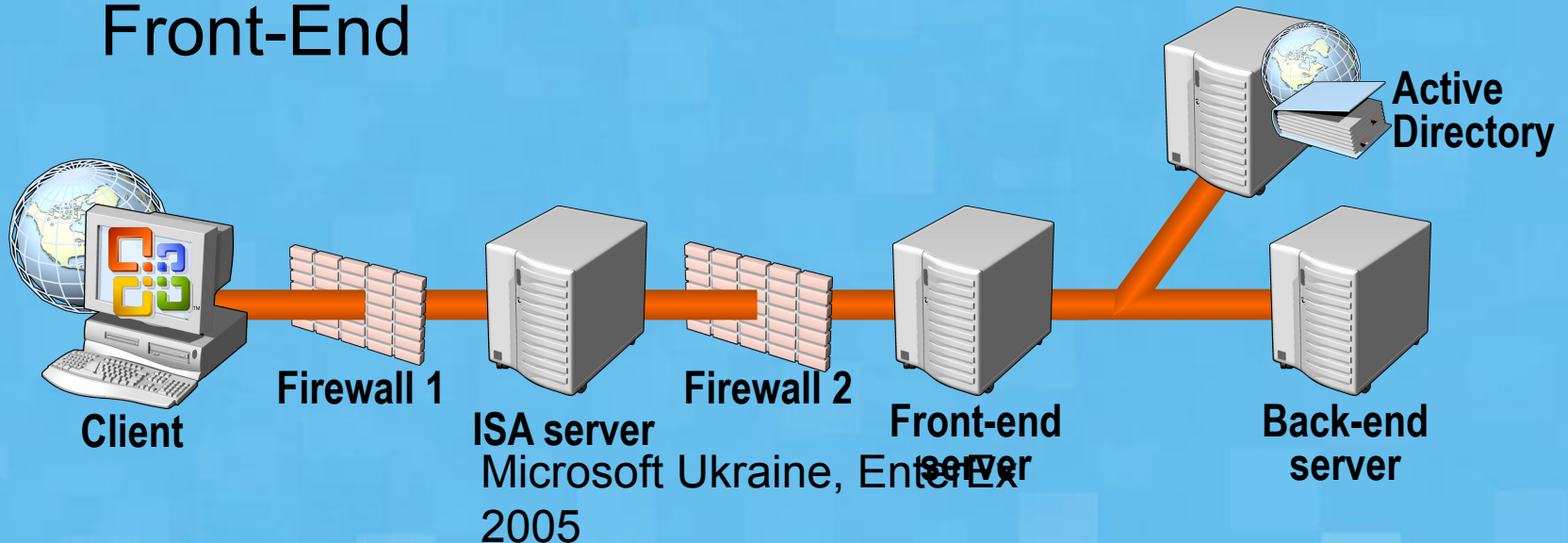
- Уязвимости кода и неверная конфигурация
  - Мониторинг возможных угроз средствами Microsoft Baseline Security Analyzer
  - Работа с информацией, предоставляемой на сайте [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) Работа с информацией, предоставляемой на сайте [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security), а также [www.microsoft.com/exchange](http://www.microsoft.com/exchange)
  - Следование рекомендациям документа «Exchange Server 2003 Security Hardening Guide»
  - Своевременная установка сервисных пакетов и требуемых заплаток средствами Microsoft Software Update Services или Microsoft Systems Management Server

# Защита от внешних угроз

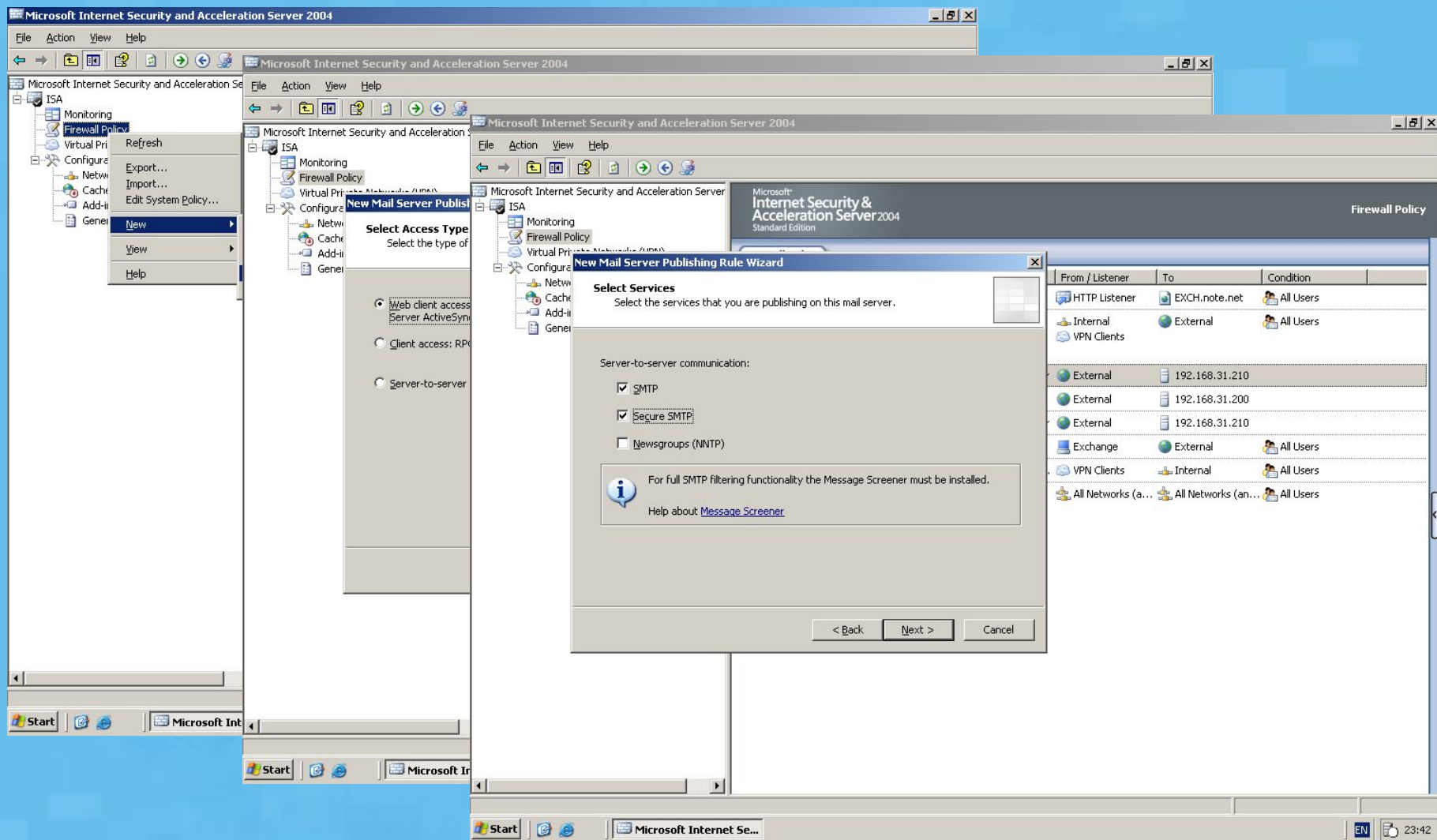
- Атаки на операционную систему
  - Защита серверов Exchange посредством создания инфраструктуры Front-End/Back-End серверов
  - Создание единой точки входа в сеть для электронных сообщений для упрощения мониторинга и обеспечения безопасности системы
  - Защита путем использования межсетевого экрана типа Microsoft ISA Server 2004 с публикацией только требуемых для работы сервера Exchange портов

# Защита от внешних угроз

- Рекомендуемая конфигурация системы
  - Firewall 1 пропускает только внешние запросы к порту SMTP (25), направленные по адресу ISA Server
  - ISA Server публикует порт SMTP сервера Front-End



# Публикация сервера SMTP средствами ISA Server 2004



2005

# Защита от внешних угроз

- Для обеспечения безопасности служб Exchange рекомендуется минимизировать количество служб
- Должны выполняться только те службы, которые требуются для обеспечения требуемой функциональности
- Возможна настройка вручную или использование рекомендаций и шаблонов политик безопасности из «Exchange Server 2003 Security Hardening Guide» для автоматизации настройки безопасности служб



# Защита от внешних угроз

- Службы, требуемые для Front-End OWA

Служба	Функциональность
Exchange Routing Engine	<b>Provides Exchange routing functionality</b>
IPSec Policy Agent	<b>IPSec filter on the Outlook Web Access server</b>
IIS Admin Service	<b>Required by MExchange routing engine</b>
World Wide Web Publishing Service	<b>Required for client communication with Outlook Web Access front-end servers</b>

# Защита от внешних угроз

- Службы, требуемые для Back-End

Служба	Функциональность
Exchange Information Store	To access mailbox and public folder stores
Exchange Management	For message tracking
Windows Management Instrumentation	For Exchange management
Exchange MTA Stacks	For Exchange maintenance to run
Exchange System Attendant	For Exchange maintenance and other tasks
Exchange Routing Engine	To coordinate message transfer between Exchange servers
IPSec Policy Agent	To implement IPSec policy on server
IIS Admin Service	For MExchange routing engine
NTLM Security Support Provider	For System Attendant
SMTP	For Exchange transport
World Wide Web Publishing Service	For communication with Outlook Web Access front-end servers

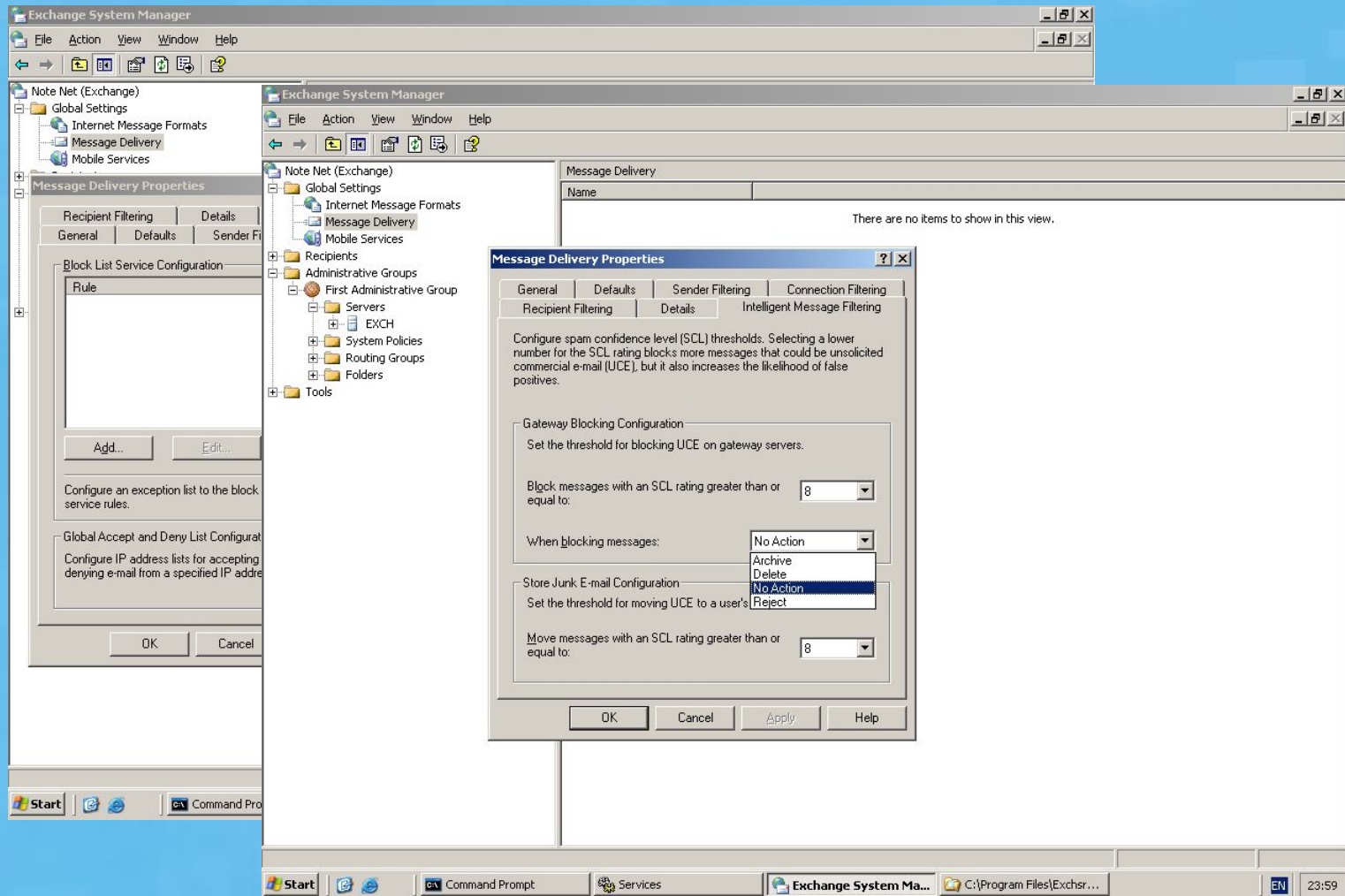
# Защита почтовых ящиков

- Требующие внимания угрозы:
  - Заполнение почтовых ящиков нежелательной почтой (спамом), что приводит к снижению производительности сервера Exchange, перерасходу дискового пространства и чрезмерному использованию каналов связи
  - Атаки на отказ обслуживания путем отправки электронных сообщений с большими вложениями
  - Попадание вирусов различных типов в почтовые ящики пользователей, обычно вместе с вложениями

# Защита почтовых ящиков

- Защита от нежелательной почты
  - Фильтрация по почтовому адресу отправителя
  - Фильтрация по адресу получателя
  - Тонкая настройка разрешений на почтовые ящики пользователей, например, с блокировкой доставки сообщений от не аутентифицированных источников
  - Фильтрация соединений с серверами SMTP по IP-адресу сервера-отправителя (block lists) на основе стандартных технологий
  - Отсев нежелательной почты по ее содержанию на основе встроенного спам-фильтра Intelligent Message Filtering, предоставляемого вместе с SP1
  - Использование нового средства Microsoft Outlook 2003 Junked E-Mail

# Настройка фильтрации нежелательной почты



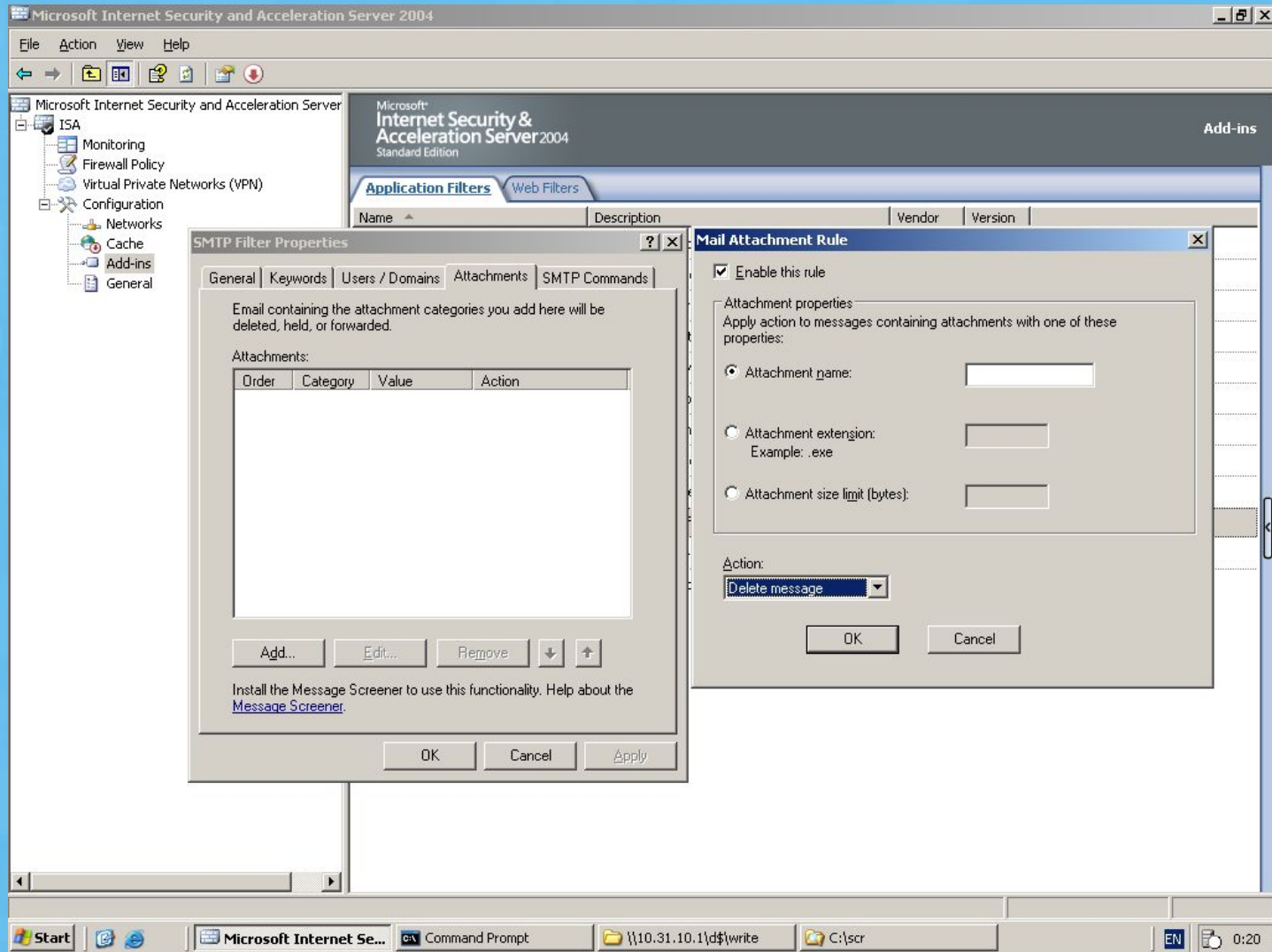
# Защита почтовых ящиков

- Защита от атаки на отказ обслуживания
  - Настройка глобальных параметров организации размера принимаемых сообщений
  - Настройка параметров отдельного Exchange SMTP Virtual Server
  - Настройка параметров почтового ящика пользователя
  - Мониторинг состояния счетчиков производительности серверов Exchange встроенными средствами, средствами ОС Windows Server или при помощи других программных продуктов, например Microsoft Operations Manager Server 2005

# Защита почтовых ящиков

- Защита от вирусов, передаваемых посредством вложений
  - Запрет открытия вложения различных типов на стороне клиента Outlook
  - Настройка работы Outlook в режиме зоны Restricted Sites и установка для этой зоны максимальных ограничений по безопасности
  - Автоматическая блокировка вложений при публикации SMTP Server средствами ISA Server с применением SMTP Filter
  - Использование антивирусных систем партнеров Microsoft, разработанных специально для использования с Exchange, а также на стороне клиентов
  - Обучение пользователей

# Настройка SMTP Filter





# Защита данных и аутентификация клиентов

- Требуемые внимания угрозы
  - Перехват конфиденциальных почтовых сообщений пользователей
  - Подделка и модификация сообщений
  - Перехват трафика при удаленной работе пользователя с Exchange по протоколам MAPI, RPC over HTTP, Outlook Web Access etc
  - Перехват аутентификации пользователя при подключении к Exchange
  - Доставка сообщений отправителей, не являющихся пользователями системы (Relay)

# Защита данных и аутентификация клиентов

- Для обеспечения конфиденциальности передачи и хранения сообщений
  - Внедрение инфраструктуры открытого ключа (PKI) для шифрования и цифровой подписи (S/MIME)
  - Использование протоколов SMTPS для безопасной передачи данных между серверами внутри и вне организации
  - Использование протокола IPSec для обеспечения безопасной работы серверов Front-end/Back-end
  - Использование встроенного режима шифрования передаваемых данных по протоколу MAPI при работе Outlook 2003
- Для обеспечения безопасного удаленного доступа и защиты аутентификации
  - Использование протоколов HTTPS, POP3S, IMAP4S, VPN соединений
  - Использование протоколов TLS для поддержки безопасной аутентификации
  - Использование Form-based режима аутентификации пользователя совместно с HTTPS для доступа к Outlook Web Access

# Настройка Relay

The screenshot displays the Exchange System Manager interface with the 'Default SMTP Virtual Server Properties' window open. The 'Connectors' list shows a '2Inet' connector of type 'SMTP Connector' last modified on 06.04.2005 at 1:10. The '2Inet Properties' dialog box is open, showing the 'General' tab. The 'Address Space' section is active, displaying a table with one entry:

Type	Address	Cost
SMTP	*	1

Below the table are buttons for 'Add...', 'Modify...', and 'Remove'. The 'Connector scope' section has 'Entire organization' selected. The 'Allow messages to be relayed to these domains' checkbox is unchecked. The taskbar at the bottom shows the Start button, Command Prompt, Services, Exchange System Manager, and a file explorer window.

# Делегирование административных привилегий

- Стандартные роли при делегировании с использованием Exchange System Manager Console
  - Exchange Full Administrator
  - Exchange Administrator
  - Exchange View Only Administrator
- Использование специальных средств ESMC и ADSIEdit для более тонкой настройки доступа к объектам Exchange

# Обеспечение высокой доступности Exchange

- Использование кластерных технологий для безостановочной работы
- Проектирование структуры групп хранения и хранилищ
- Резервное копирование и навыки восстановления
- Использование специальных функций восстановления (Recovery Storage Group & Recovery Mailbox Data Wizard) и утилит для обслуживания хранилищ (eseutil, isinteg)
- Мониторинг ресурсов (свободная память, дисковое пространство), показателей производительности, работоспособности и доступности служб и коннекторов
- 90% сбоев Exchange – отсутствие свободного дискового пространства