Политика управления обновлениям

Виды исправлений ПО Microsoft

Service Packs

Hot Fixes

(оперативные обновления)

Security Patches

(обновления безопасности)

Политика управления обновлениями

1. Инвентаризация программных продуктов

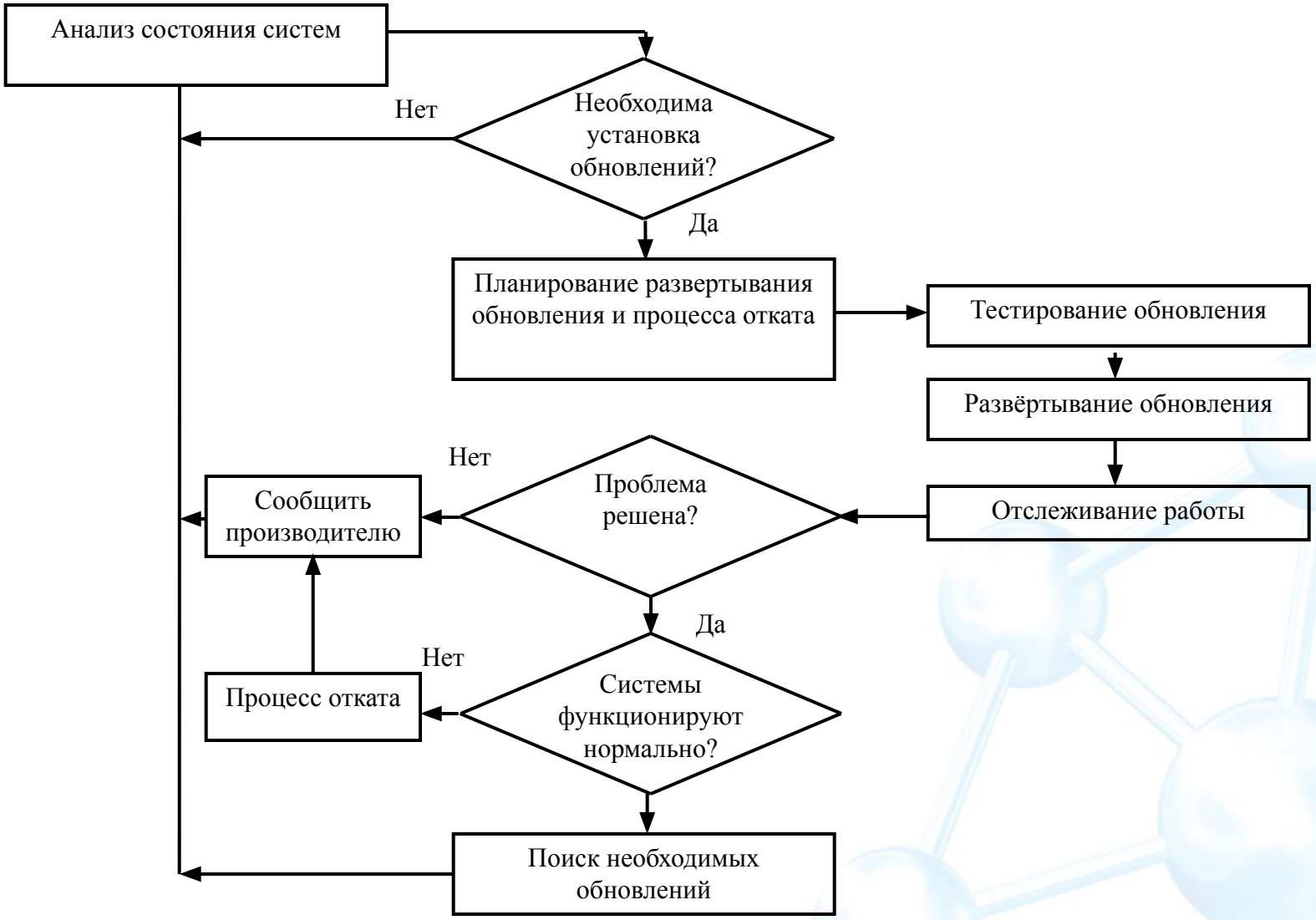
2. Категорирование программных продуктов

3. Закрепление лиц, ответственных за обновление ПО

4. Закрепление лиц ответственных за контроль установки обновлений ПО

5. Выбор технических средств

Политика управления обновлениями



Информация об уязвимостях и обновлениях

Microsoft Product Security Notification Service

Рассылка производится по мере выхода обновлений и содержит общее
описание проблемы и ссылку на статью базы знаний Microsoft, содержащую подробную информации об обновлении.

http://www.microsoft.com/technet/security/notify.asp

NT BugTraq

Модерируемый публичный список рассылки содержащий информацию
об уязвимостях операционных систем Windows и продуктов Microsoft,
а так же рекомендации по их устранению.

http://www.ntbugtraq.com

SecurityFocus

Содержит наиболее полный и оперативно обновляемый список уязвимостей для различных операционных систем. Зачастую в данном списке публикуются информация о не закрытых уязвимостях.

http://www.securityfocus.com

Утилита Hfnetchk

Утилита командной строки

Поддерживает **удаленную** и локальную проверку установленных обновлений ПО

Проверяемые продукты

- ОС Windows NT, Windows 2000 и Windows XP
- Стандартные сервиса (включая IIS)
- Windows Media Player
- Internet Explorer
- MDAC
- MS SQL Server 7.0-2000
- MS Exchange 5.5-2000

Проверяет версии файлов

Постоянно обновляемый список требуемых обновлений

Microsoft Baseline Security Analyzer

Использует технологию hfnetchk

Поддерживает GUI и CLI интерфейс (**mbsacli.exe**)

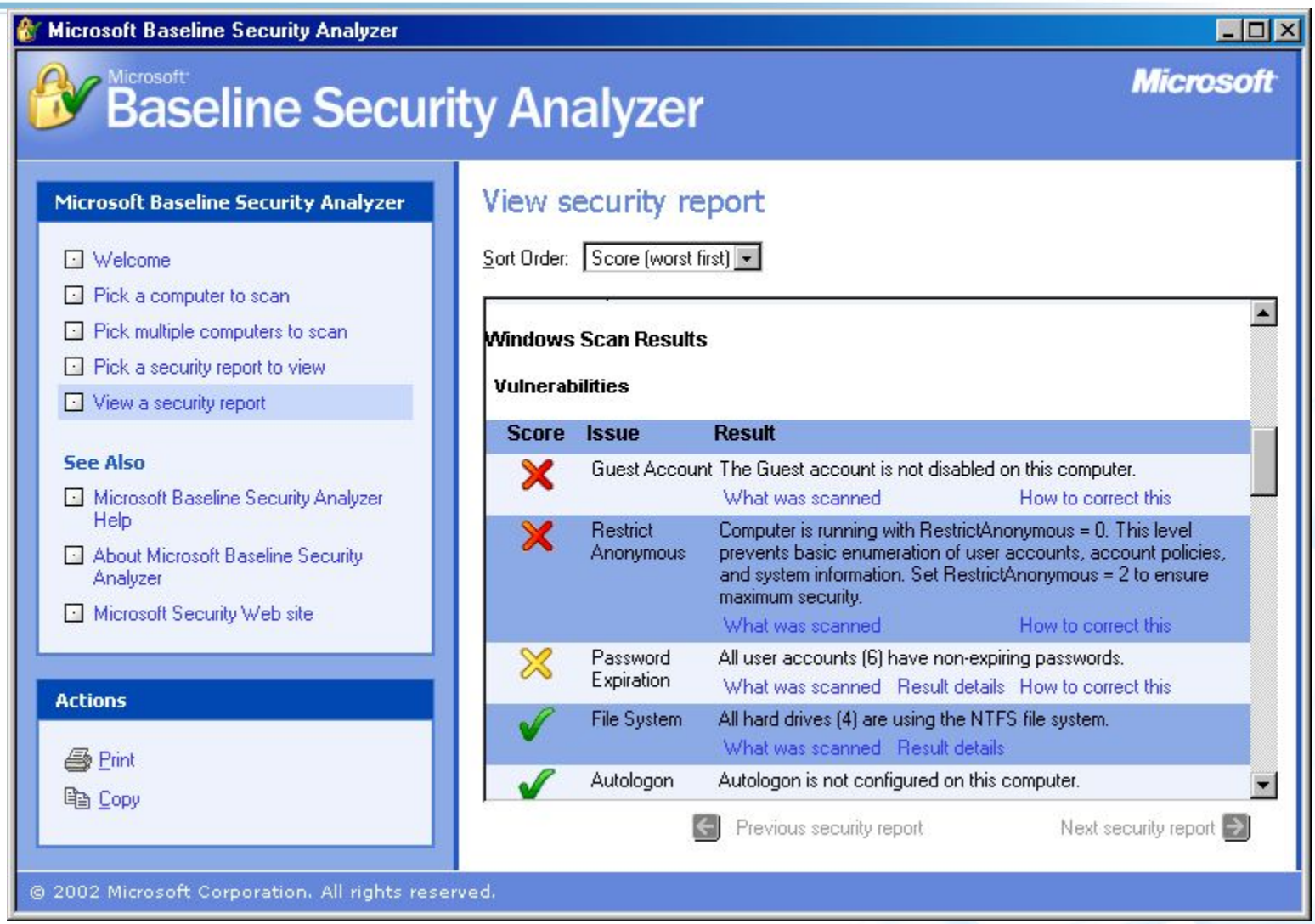
Не проверяет установленные обновления для MDAC

Не работает на Windows NT 4.0

Имеет возможность получения списка необходимых обновлений с сервера **Microsoft Software Update Services**

Проверка основных ошибок в настройке операционной системы

Microsoft Baseline Security Analyzer



Установка обновлений (Service Packs)

Установка обновлением

Традиционный метод обновления операционных систем Windows NT и Windows 2000

Интегрированная установка

Интеграция файлов пакета обновлений в исходный дистрибутив Windows 2000

Комбинированная установка

Установка обновлений безопасности

q294391_w2k_sp3_x86_en.exe

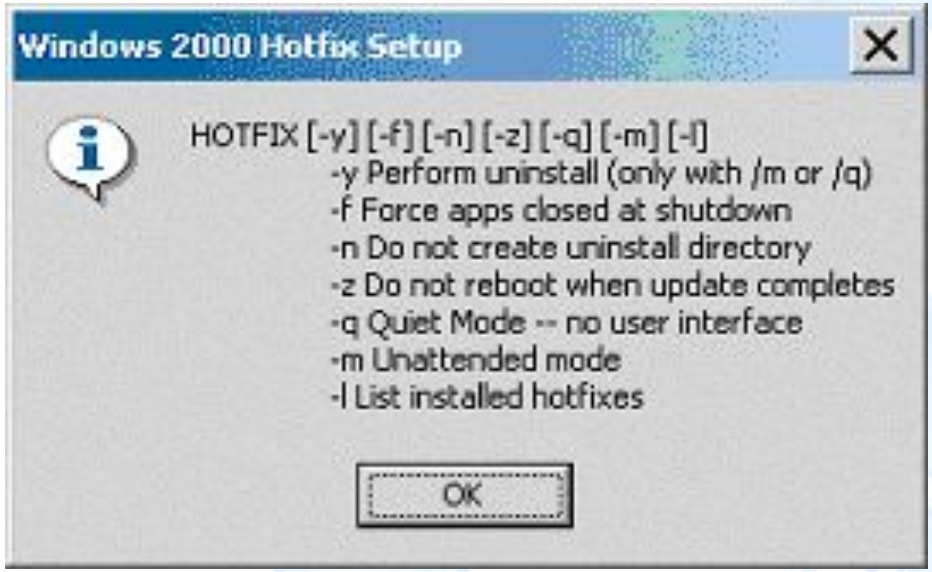
Номер статьи Microsoft KB

Описание устраняемой уязвимости. Условия применения и т.д.

Операционная система

Пакет обновлений, в которые данное обновление будет включено

Аппаратная платформа и язык



Установка обновлений безопасности

Установка цепочек обновлений

Одновременная установка нескольких обновлений при помощи одного файла сценария

Установка через групповые политики

Централизованная установка обновлений через GPO в среде Active Directory

Software Update Services и Update Client

Полностью автоматизированная система централизованного управления обновлениями

Установка обновлений (Service Packs)

Software Update Services

Автоматическое получение обновлений с сервера Windows Update

Автоматическая установка обновления на клиентские места

Своевременное информирование администратора о выходе обновлений

Поддержка параллельной (Load Balancing) и последовательной схемы распределения нагрузки

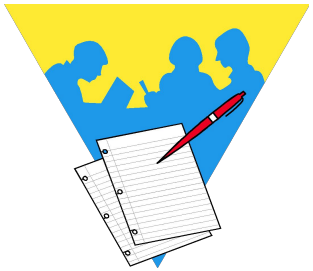
Работа в сетях не подключенных к Internet

Отсутствует возможность указать список используемых продуктов

Не поддерживает обновления для MS OFFICE, серверных приложений

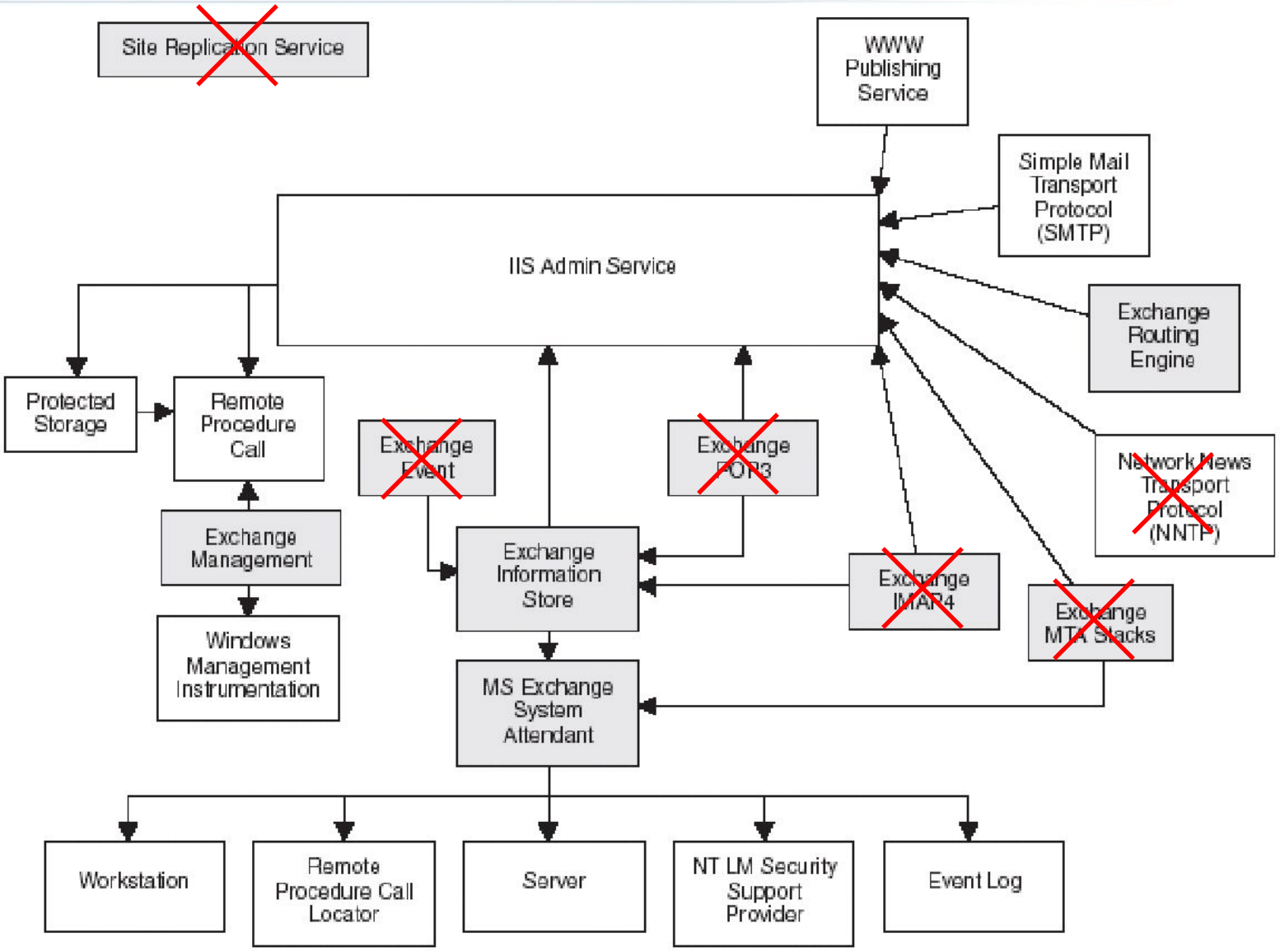
Практическая работа 7

Работа с утилитой MBSA



Настройка компонентов Exchange

Взаимосвязь компонентов сервера



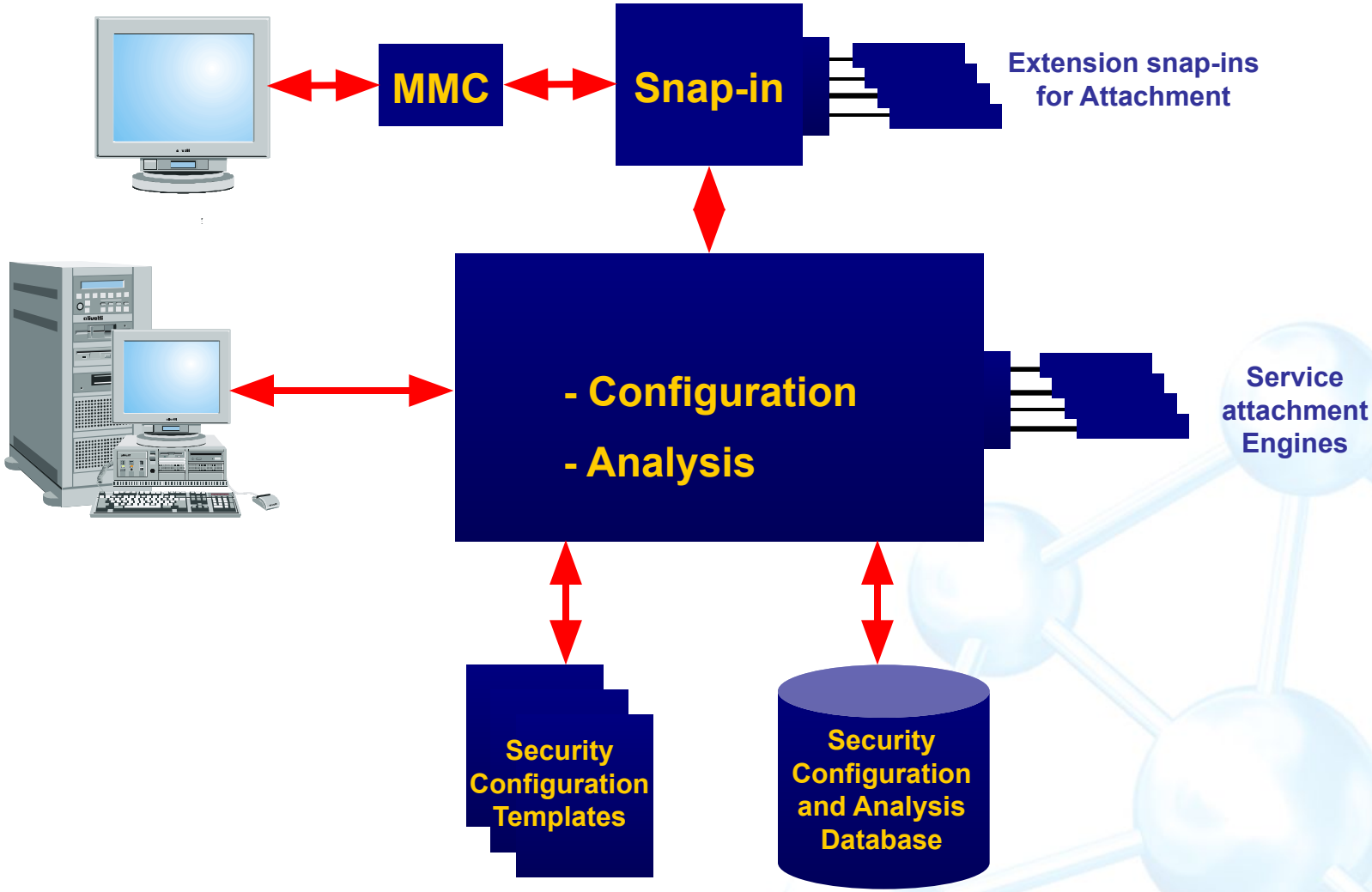
Службы сервера Exchange

Сервис	Состояние	Причина
Microsoft Exchange IMAP4	Отключен	В связи с невысокой степень защищенности коммуникаций
Microsoft Exchange NNTP	*Отключен*	*Не требуется для обеспечения базовой функциональности. Может включаться при необходимости.*
Microsoft Exchange POP3	Отключен	В связи с невысокой степень защищенности коммуникаций
Microsoft Exchange Search	Отключен	Не требуется для обеспечения базовой функциональности. Может включаться при необходимости.
Microsoft Exchange Event Service	Отключен	Требуется только для совместимости с приложениями Exchange 5.5
Microsoft Exchange Site Replication Service	Отключен	Требуется только в смешанной среде (Exchange 5.5/2000)
Windows Installer	*Отключен*	*Необходим только во время установки дополнительного ПО*
Distributed Transaction Coordinator	*Отключен*	*Не требуется для обеспечения базовой функциональности*

Разрешения файловой системы

%systemdrive%\Inetpub\mailroot	Domain Admins: Full Control Local System: Full Controll
%systemdrive%\Inetpub\nntpfile	Domain Admins: Full Control Local System: Full Controll
%systemdrive%\Inetpub\nntpfile\root	Everyone: Full Control

Security Configuration Tool Set



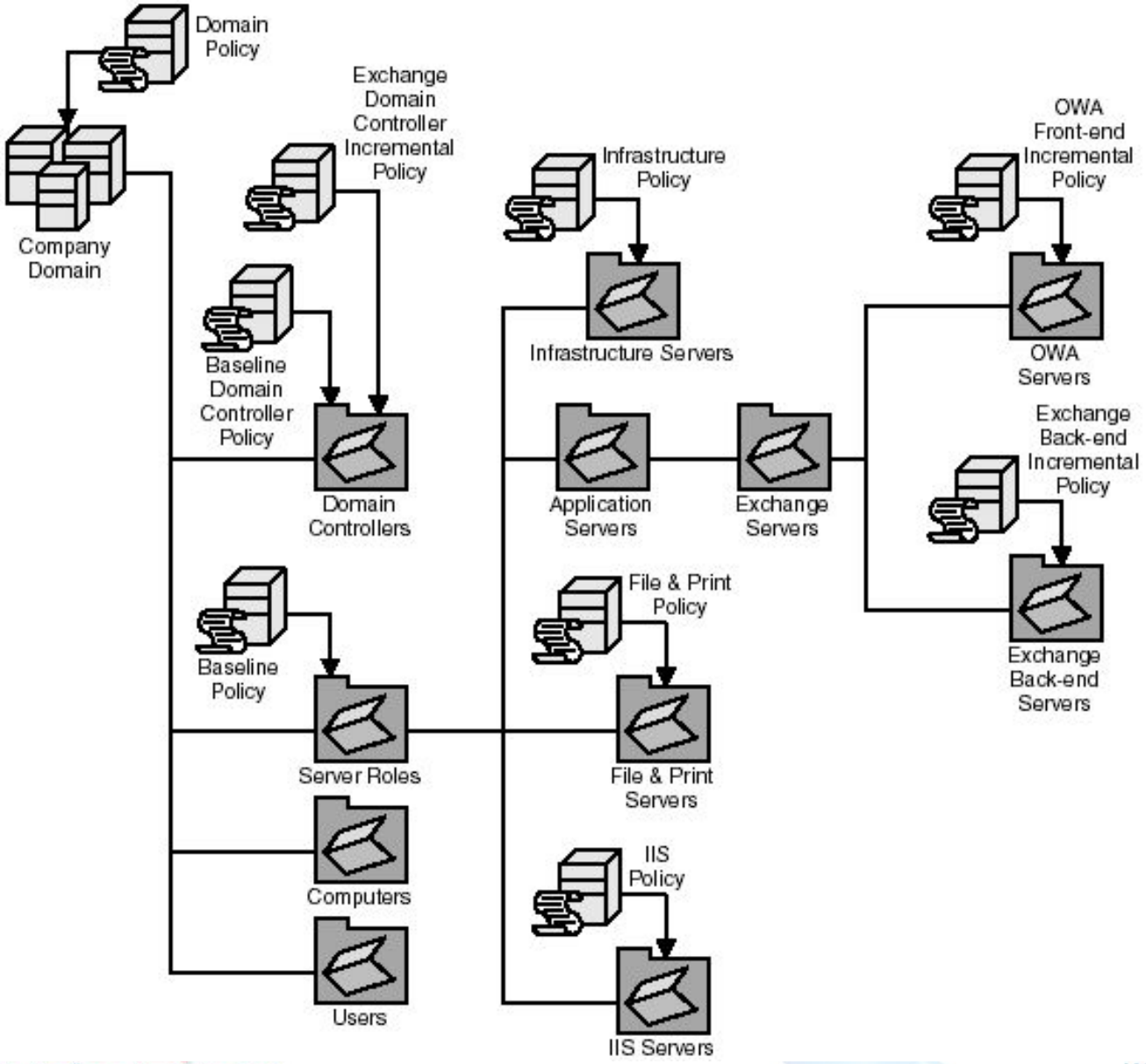
Шаблоны безопасности

Использование

Secedit может использоваться для пяти основных операций

Анализ	**Системы безопасности**
Настройка	**Системы безопасности**
Экспорт	**Параметров безопасности**
Обновление	**Параметров безопасности**
Проверка	**Файла конфигурации безопасности**

Применение шаблонов безопасности



Делегирование полномочий

Делегирование полномочий

Роли администраторов Exchange

Exchange View Only

просмотр значений свойств объектов

Exchange Administrator

просмотр и изменение значений свойств объектов

становиться владельцем, изменять разрешения, открывать почтовые ящики

Exchange Full Administrator

все разрешения, включая и изменение разрешений

открывать почтовые ящики

Делегирование полномочий

Применение прав

Exchange Administration Delegation Wizard

Вкладка Security для контейнеров

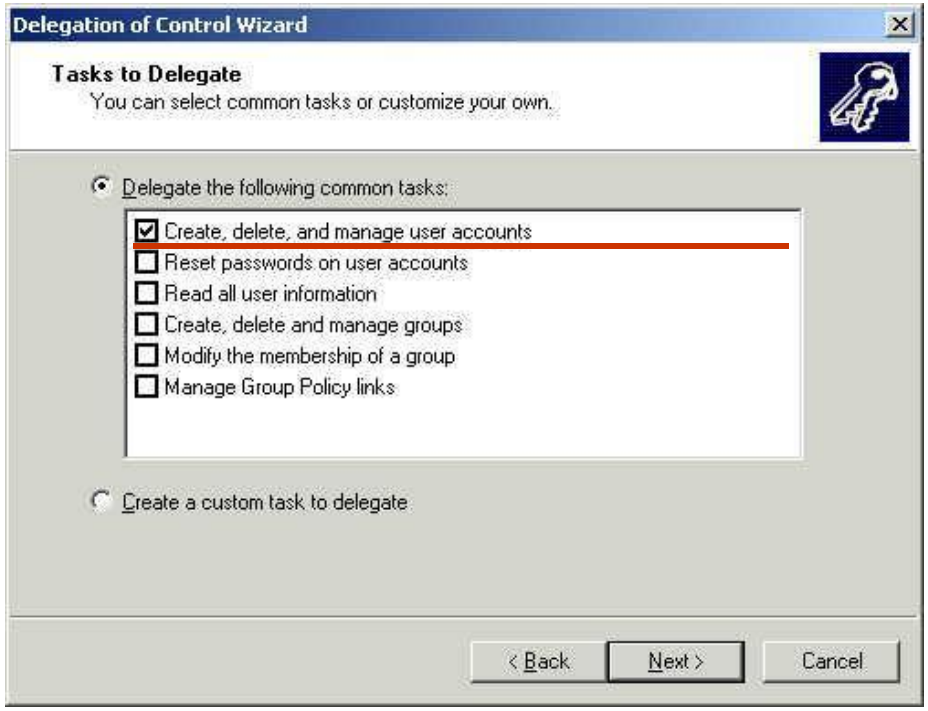
- Address Lists
- Global Address Lists
- Databases (Mailbox Stores и Public Folder stores)
- На верхнем уровне иерархи общих папок

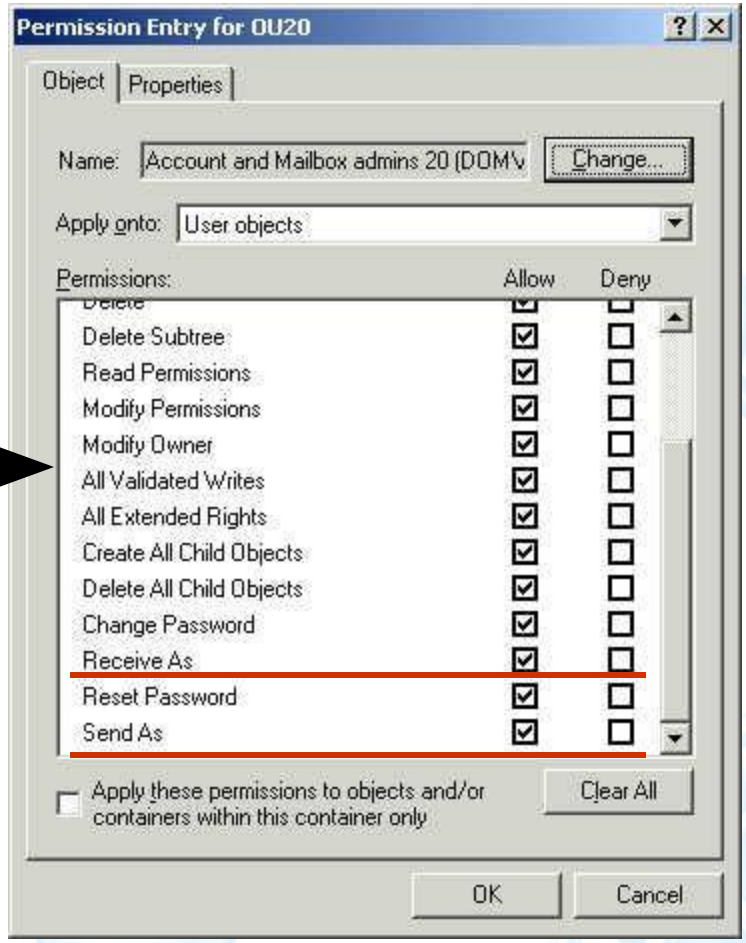
HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin\ ShowSecurityPage=1

Делегирование полномочий

Делегирование задач на уровне OU

Exchange View Only + Мастер делегирования AD





Системная политика

Позволяет централизованно настраивать параметры групп серверов

Перекрывает настройки, сделанные вручную

Позволяет подчинять действия администраторов серверов политике предприятия

Системная политика

Шаблоны политики

Server Policy

Public Store Policy

Mailbox Store Policy

Системная политика

Server Policy

General

- Enable subject logging and display
- Enable message tracking
- Remove log files

Системная политика

Mailbox Store Policy

General

- Default public store for users
- Offline Address List for users
- Archive all messages

Database

- Run maintenance during this time

Limits

- Delete after (days)
- Don't permanently delete items until back up
- Issue warning at (KB)
- Prohibit send at (KB)
- Prohibit send and receive at (KB)
- Send over-limit messages

Системная политика

Public Store Policy

General
- Clients support S/MIME signatures
- Display inbound Internet messages in fixed font

Database
- Run maintenance during this time

Replication
- Replicate public folder changes
- Replication interval for always (minutes)
- Replication message size limit (KB)

Limits
- Delete after (days)
- Don't permanently delete items until backed up
- Issue warning at (KB)
- Send over-limit messages
- Age limit for all folders in this store (days)

edslock.vbs

Члены группы Exchange Domain Servers имеют доступ ко всем объектам серверов Exchange

Члены группы Account Administrators имеют возможность добавить учетные записи в группу Exchange Domain Servers

Таким образом, получают право «Receive As», т.е. возможность работы с почтовыми ящиками всех пользователей в домене!

edslock.vbs

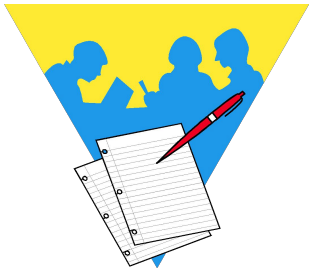
Утилита edslock.vbs (MS KB Q313807) устанавливает разрешение Deny Receive As на объектах сервера

Необходимо применять:
После установки нового сервера Exchange 5.5
После добавления нового хранилища Public Folders
После добавления нового хранилища Mailbox
После добавления в лес нового домена

cscript edslock.vbs "CN=Mail1,CN=Servers,CN=America AG,CN=Administrative Groups,CN=Microsoft, CN=Microsoft Exchange,CN=Services,CN=Configuration, DC=America,DC=microsoft,DC=com

Практическая работа 9

Делегирование полномочий



Вопросы ?