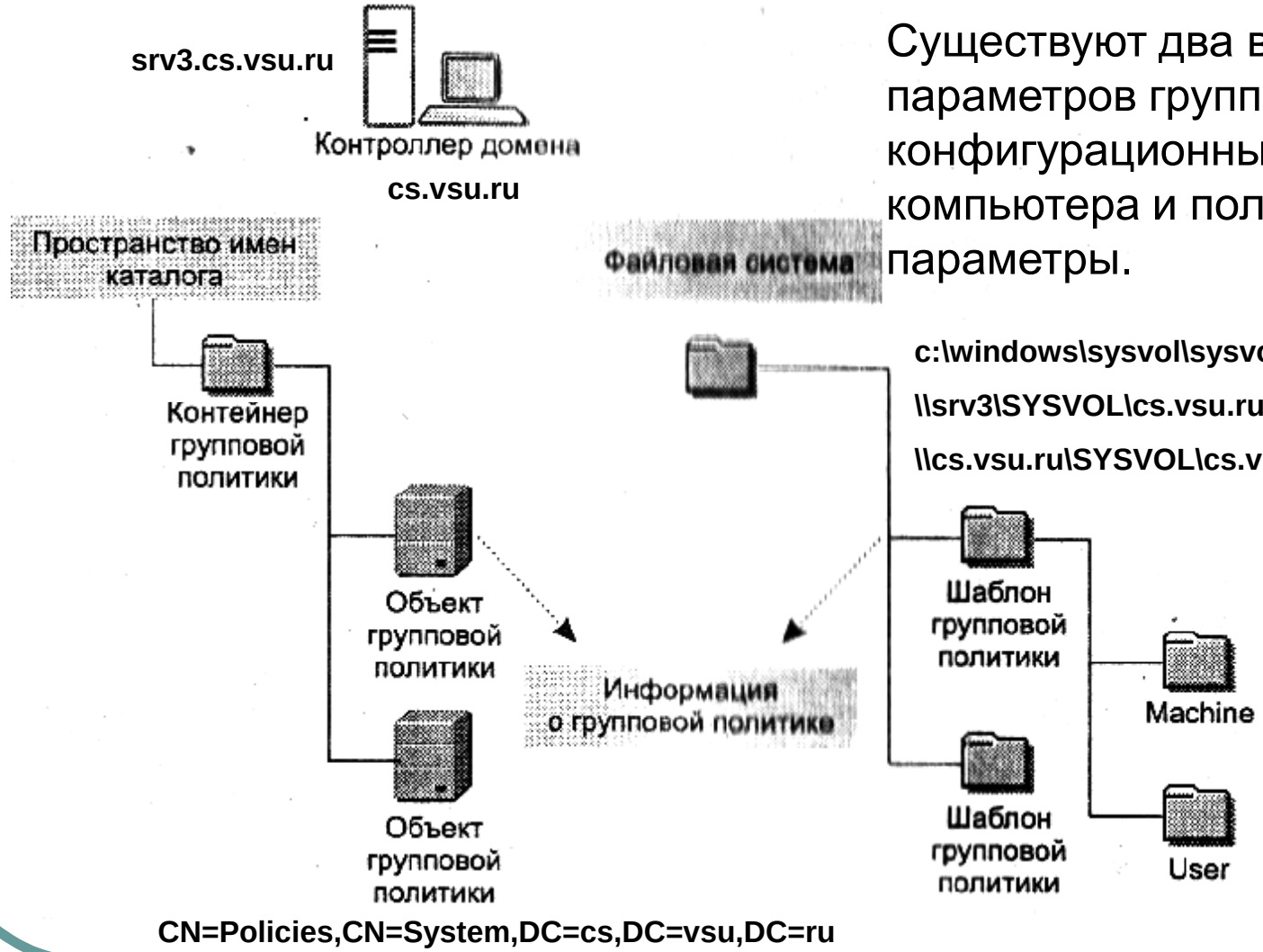
Объекты групповой политики

- Объекты групповой политики (GPO – Group Policy Objects) представляют собой набор конфигурационных параметров операционной системы и ее приложений.
- Существуют два типа GPO:
  - AD GPO могут быть ассоциированы с объектами каталога контейнерного типа:
    - домен
    - организационная единица
    - сайт
  - Локальные GPO – хранятся на каждом компьютере. Поддерживают сокращенный набор настроек, имеют наименьший приоритет, если компьютер включен в домен.
    - %systemroot%\system32\GroupPolicy

Хранение элементов GPO

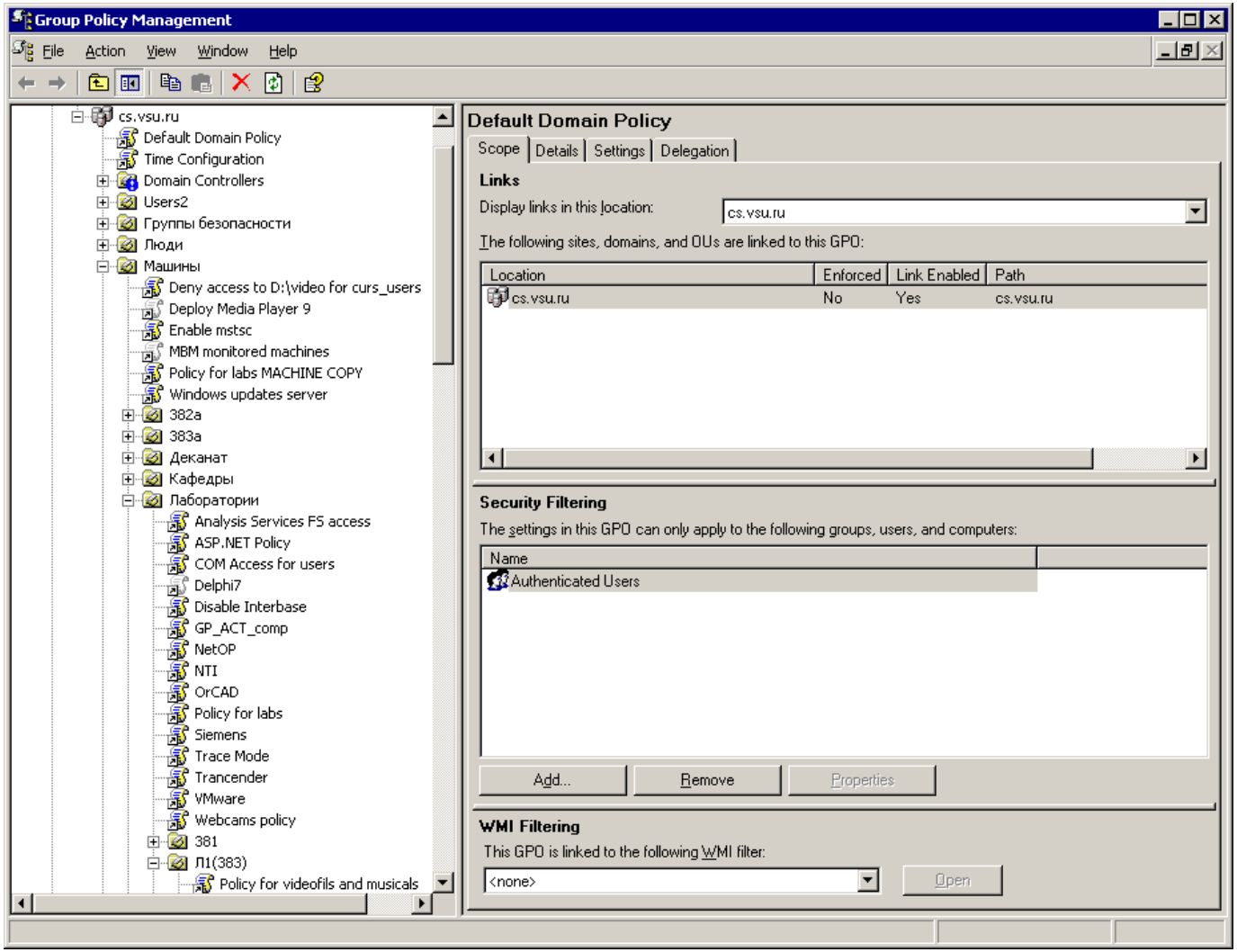


Существуют два вида параметров групповой политики: конфигурационные параметры компьютера и пользовательские параметры.

Порядок применения GPO

- GPO уровня узла
- GPO уровня сайта
- GPO уровня домена
- GPO уровня организационных единиц
- На порядок применения можно влиять с помощью запрещения наследования (Block Inheritance) для домена или OU, запрещения перекрытия (No override, enforced) и замыкания на себя (loopback, элемент политики: UserGroupPolicyLoopbackProcessingMode в Computer Configuration\Administrative Templates\System\Group Policy).
- Кроме того, применением GPO можно управлять с помощью т.н. “Security filtering”

Иерархия GPO



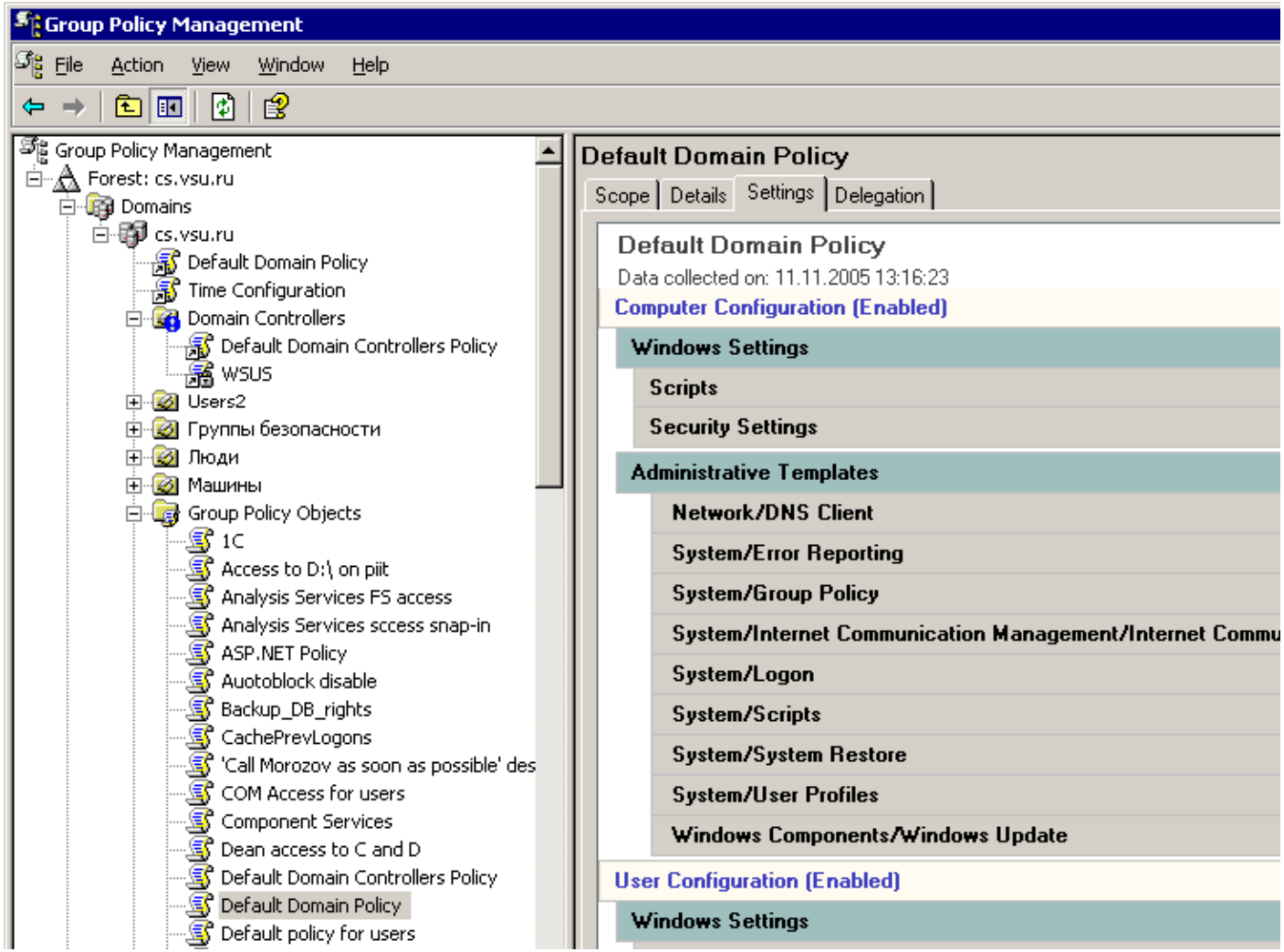
Наследование параметров GPO

- Наследуются параметры, которые определены для родительского контейнера, но не определены для дочернего
- В случае множества значений параметра, настройки родительского GPO дополняют GPO дочернего

Последовательность применения политик при загрузке ОС и входе пользователя

- Запуск службы MS RPC
- Загрузка списка GPO с DC
- Применение конфигурационных параметров в порядке: локальный GPO, GPO сайта, GPO домена, GPO подразделения
- Выполнение сценариев (по-умолчанию таймаут 10 минут)
- Приглашение ко входу в систему, вход
- Загрузка списка GPO пользователя
- Применение конфигурационных параметров пользователя
- Отображается пользовательский интерфейс

Управление групповой политикой

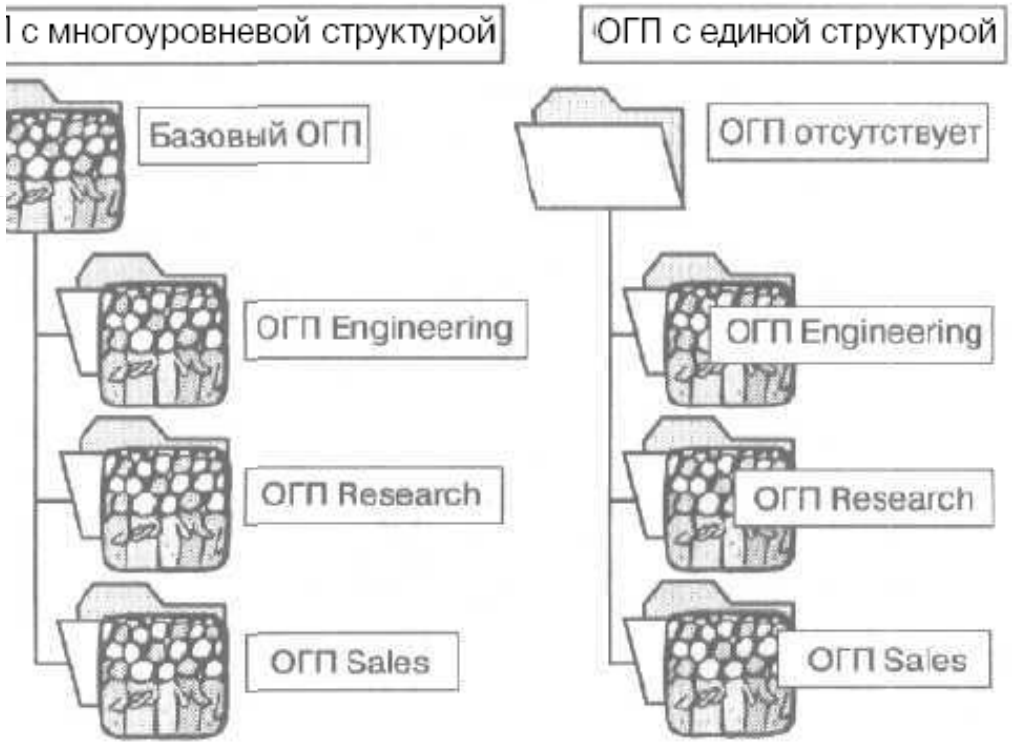


Схемы организации GPO

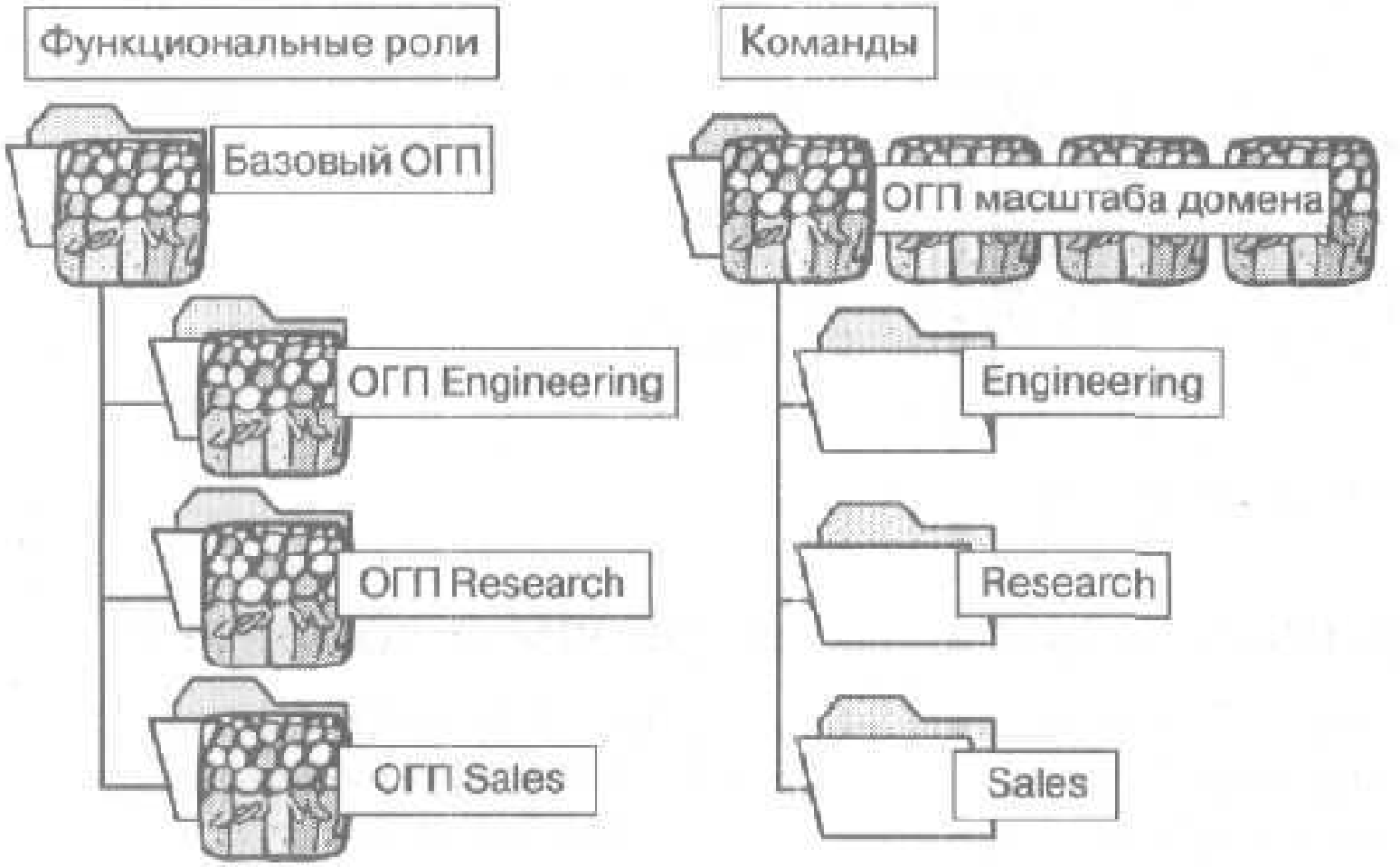
- Однородная
- Комбинированная
- Раздельная

Многоуровневая и единая структура ОГП

Могут использоваться различные стратегии по организации GPO: **многоуровневая** (хранение централизованное) и **единая** (хранение распределенное) структура ОГП

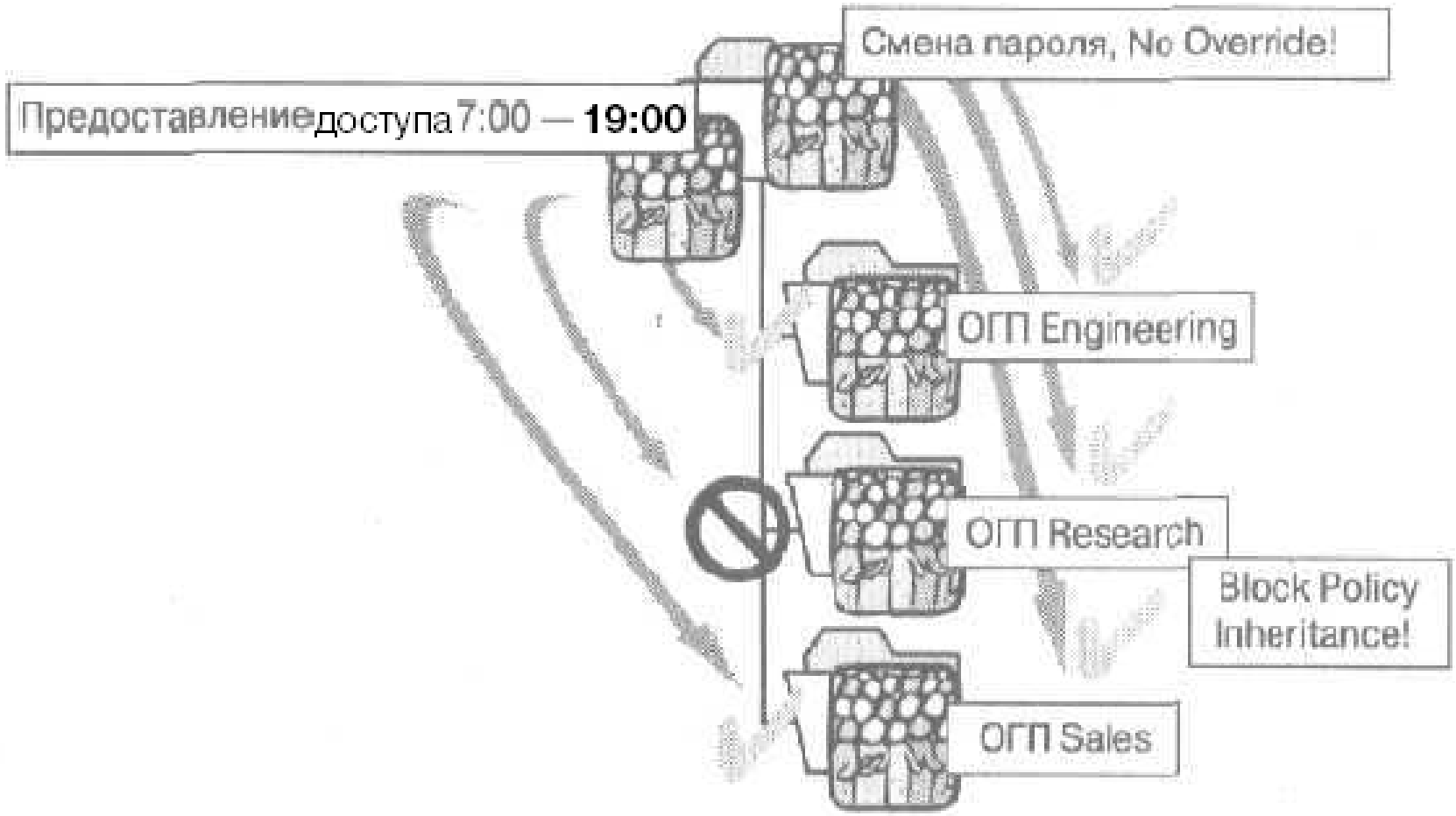


Структурирование GPO по ролям и командам



Вариант «… по командам» используется совместно с security filtering

Делегирование полномочий на администрирование GPO



Расположение параметров политик

- Реестр (registry) – иерархическая БД, состоящая т.н. «ульев» или «кустов» (англ. hives)
- Куст содержит ключи, под-ключи и значения параметров
- Каждый куст содержится в файле %***systemroot%***\config
- Редактируется программой regedit

Административные шаблоны (Administrative Templates)

- Административный шаблон представляет собой текстовый файл *.adm (на языке ADM) в Unicode и хранится в папке %SystemRoot%\inf (например, system.adm). Файл содержит перечисление ключей и параметров реестра.
- AT позволяют администратору посредством групповой политики конфигурировать hives HKLM и HKCU системного реестра компьютеров домена.
- **Обычно** используются ветви HKLM\Software\Policies (управление параметрами компьютера) и HKCU\Software\Policies (управление средой пользователей).
- \Policies очищаются системой при каждом применении или отзыве объекта групповой политики. В случае, когда компьютер не подпадает под действие ни одного объекта групповой политики, для настройки системы используются стандартные значения параметров, определенных в соответствующих ключах реестра.

Дополнительные (альтернативные) ветви реестра:
(HKLM, HKCU)\Software\Microsoft\Windows\CurrentVersion\Policies

Поставляемые шаблоны (каталог %SystemRoot%\inf) с ОС W2K3

Common.adm	Административный шаблон, используемый для настройки параметров системы на Windows 9x/NT-клиентах
Conf.adm	Административный шаблон, используемый для настройки NetMeeting
Inetcorp.adm	Административный шаблон, используемый для настройки браузера Internet Explorer для работы в корпоративной среде
Inetres.adm	Административный шаблон, используемый для настройки ограничений браузера Internet Explorer
Inetset.adm	Административный шаблон, используемый для настройки браузера Internet Explorer
System. adm	Административный шаблон, используемый для настройки различных параметров системы
Windows. adm	Административный шаблон, используемый для конфигурирования Windows Эх-клиентов
Winnt.adm	Административный шаблон, используемый для конфигурирования Windows NT-клиентов
Wmplayer.adm	Административный шаблон, используемый для настройки приложения Windows Media Player
Wuau.adm	Административный шаблон, используемый для настройки службы автоматического обновления

Шаблоны безопасности

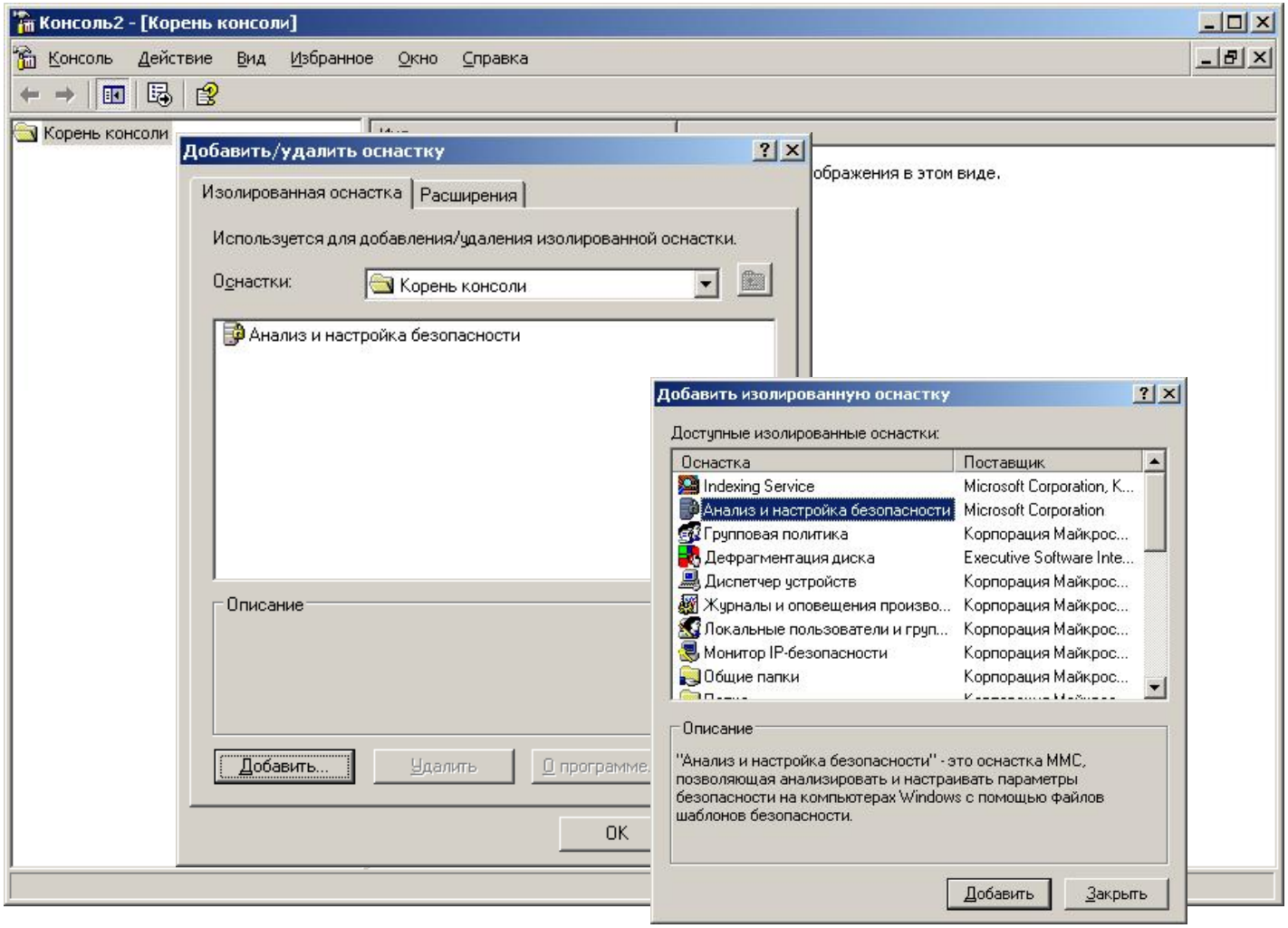
- Шаблоны безопасности позволяют создавать типовые профили безопасности, соответствующие требованиям организации
- Для формирования шаблонов используется консоль «Анализ и настройка безопасности» и готовые шаблоны из %windir%\Security\Templates
- Затем шаблон можно импортировать в компонент групповой политики «Параметры безопасности»

Работа с шаблонами безопасности

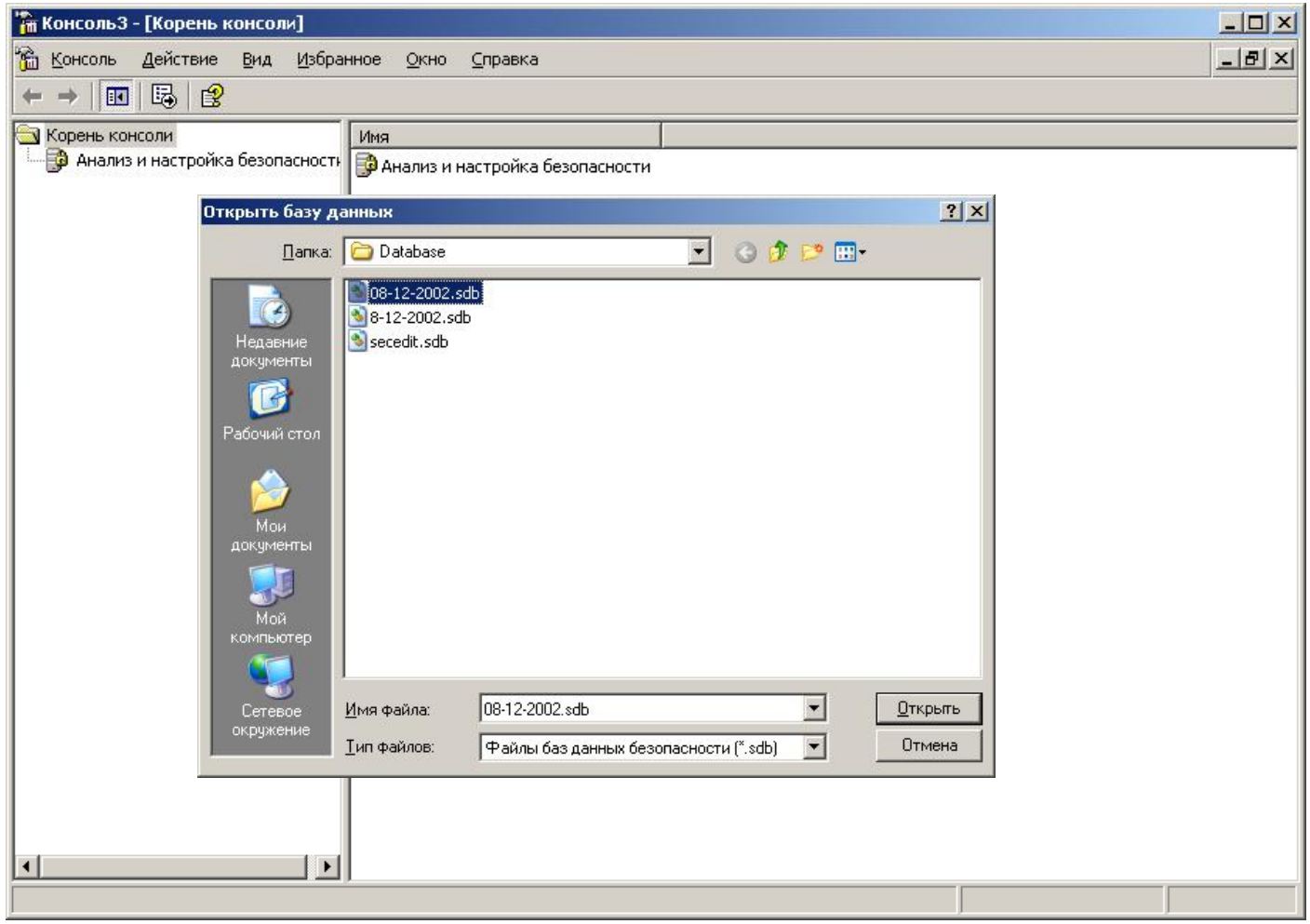
Работа с шаблонами групповых политик обычно выполняется в следующей последовательности:

- подготавливаются необходимые шаблоны безопасности;
- создается БД безопасности;
- применяются шаблоны безопасности: используются: утилита secedit, консоль «Анализ и настройка безопасности» или групповая политика;
- secedit /generaterollеback – шаблон отката

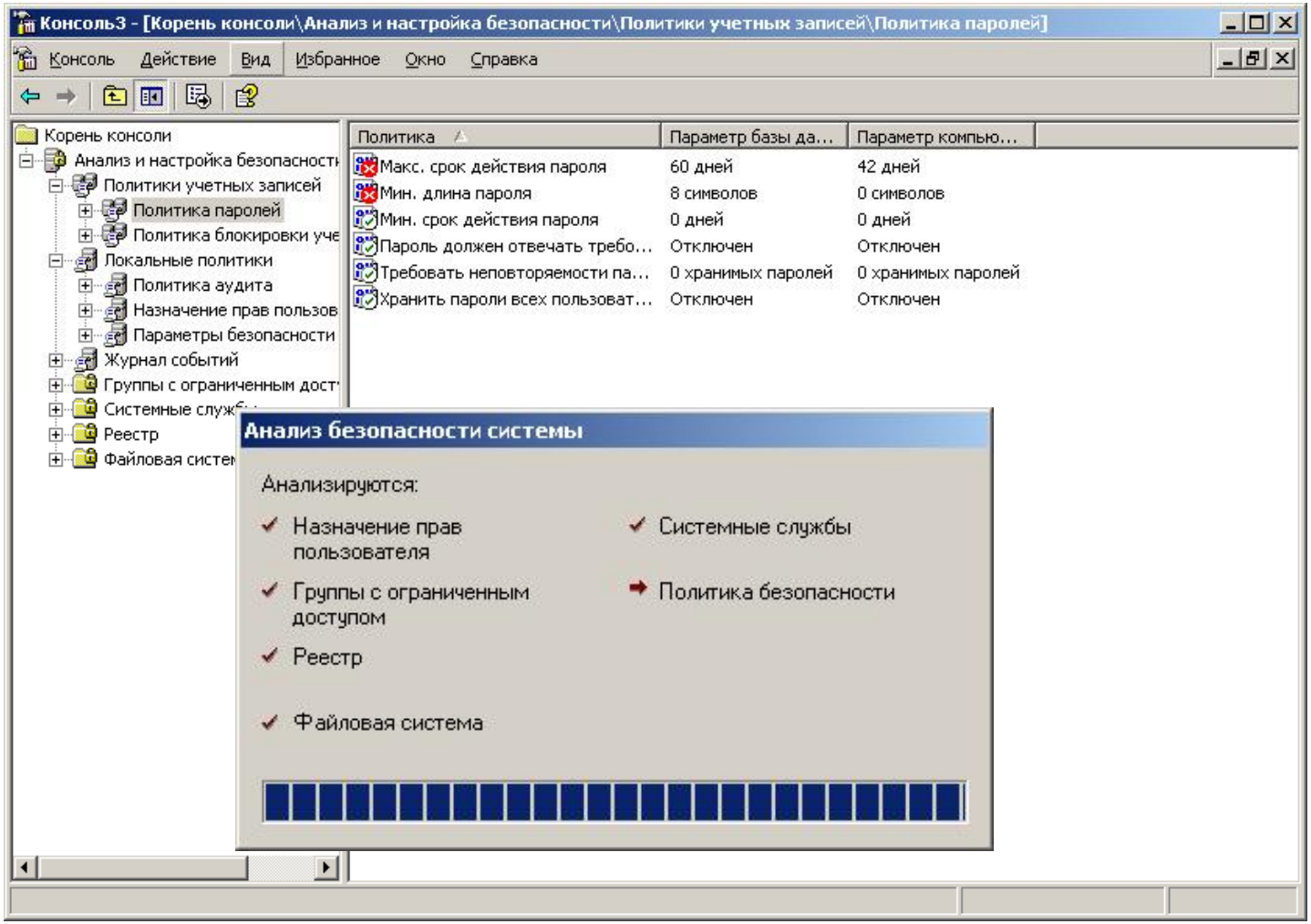
Создание консоли «Анализ и настройка безопасности»



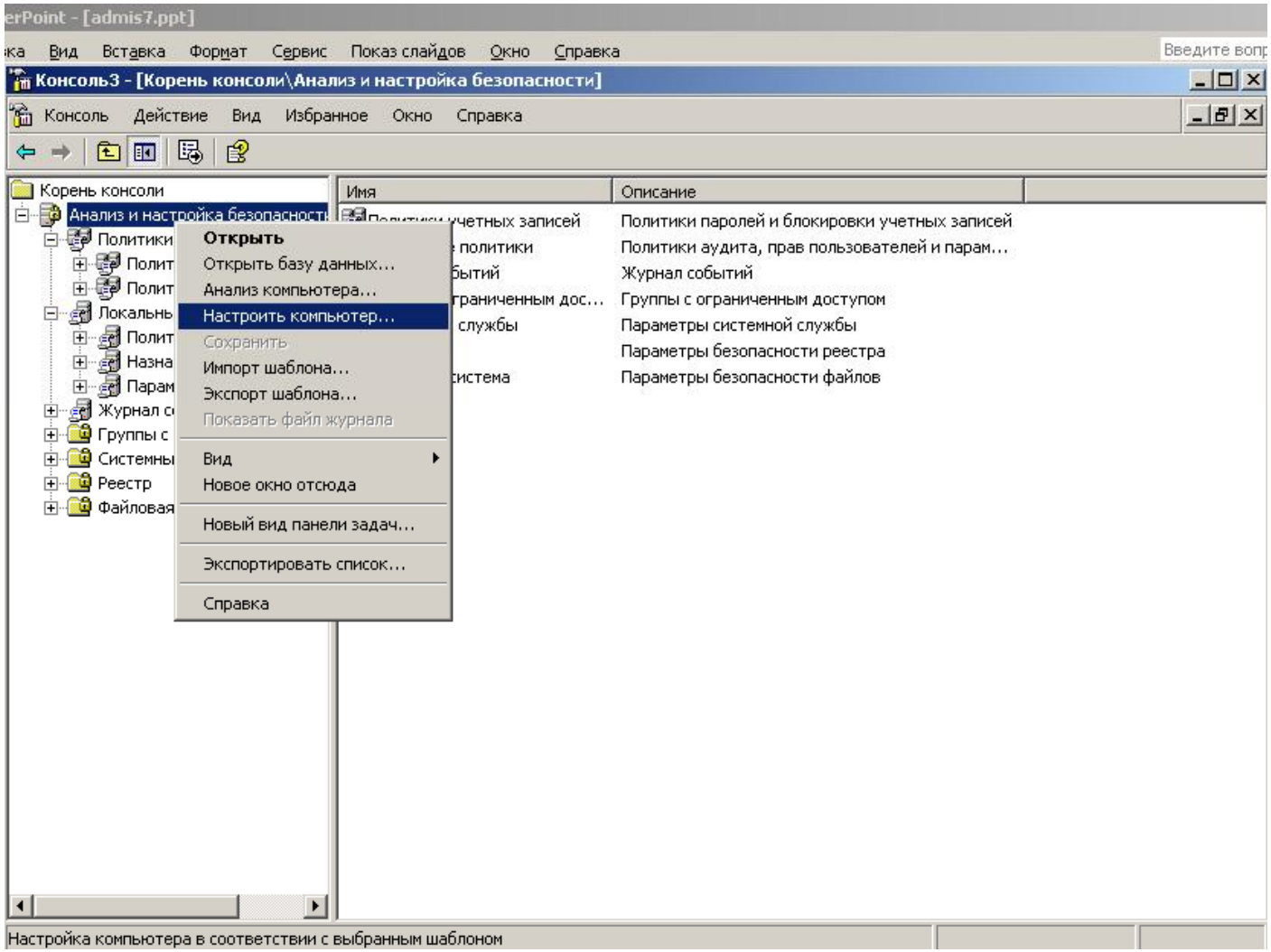
Создание новой БД безопасности



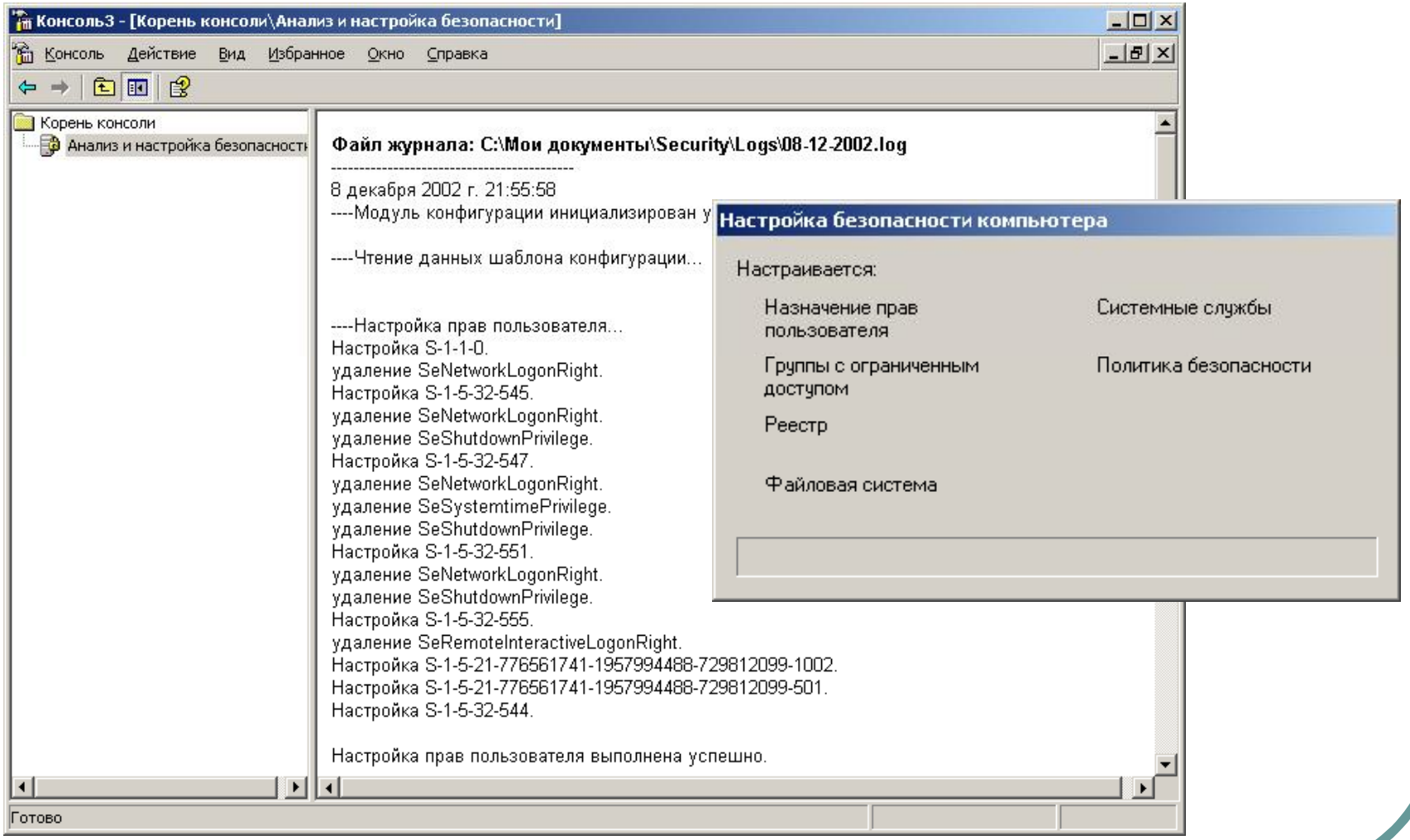
Сопоставление текущей политики безопасности с шаблоном, анализ



Применение политики



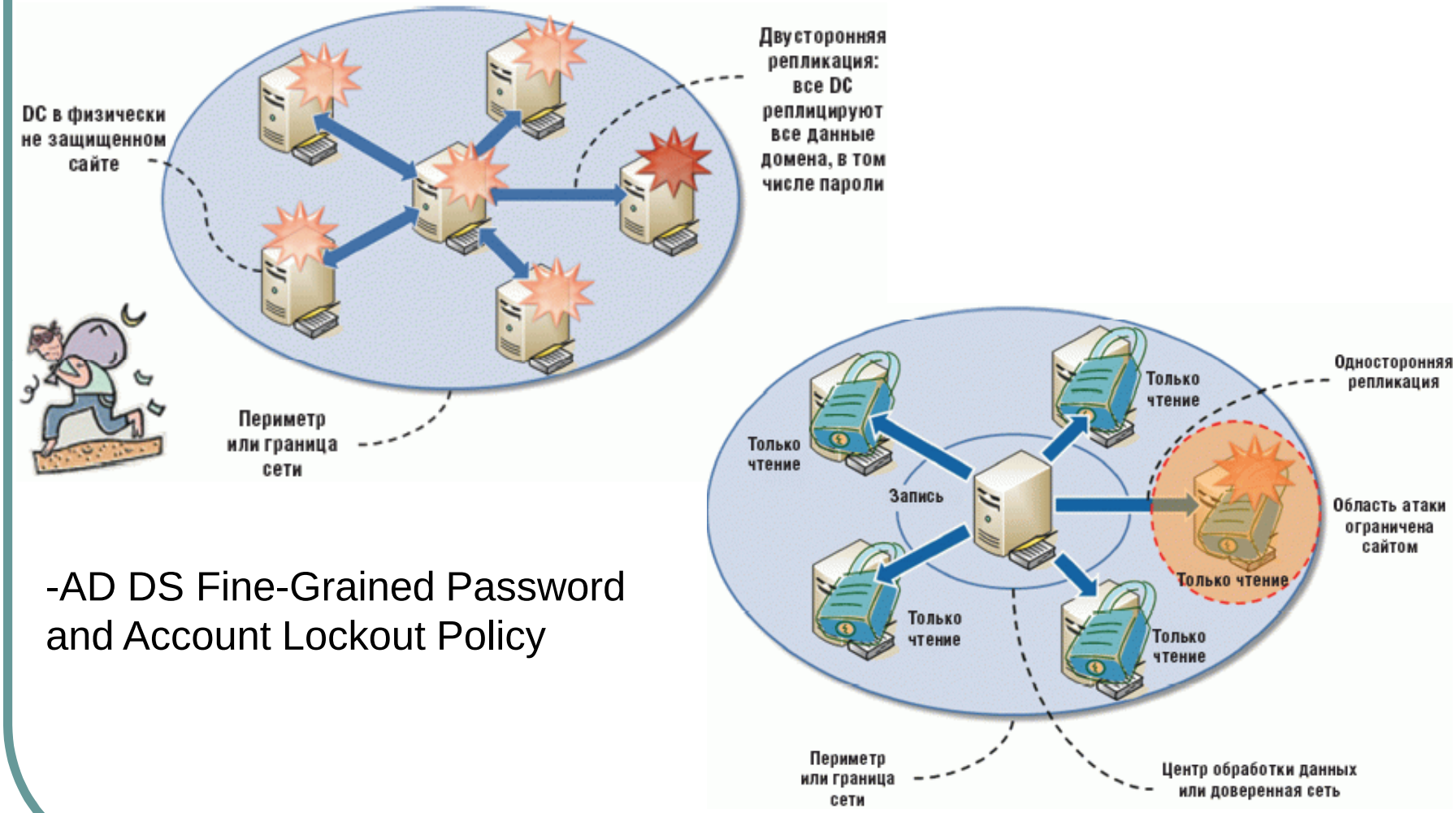
Журнал применения политики



MS IntelliMirror

- Возможности IntelliMirror (набор технологий управления ИТ-инфраструктурой снижающих т.н. стоимость эксплуатации (total cost of ownership, TCO))
  - Управление данными (Data Management)
    - перенаправление каталогов (Folder Redirection)
    - автономные файлы (Offline Folders)
    - дисковые квоты
  - Управление пользовательскими параметрами настройки (Desktop Settings Management)
  - Установка и сопровождение ПО (Software Installation and Maintenance)
  - Службы удаленной установки (RIS)
- Технологии, входящие в состав IntelliMirror
  - Служба каталогов Active Directory
  - Групповая политика Group Policy
  - Перемещаемые профили пользователя Roaming User Profiles
  - Перенаправление каталогов Folder Redirection
  - Автономные файлы Offline Folders

Развитие AD, RODC



-AD DS Fine-Grained Password and Account Lockout Policy

Изменения в Server 2008

- Режимы совместимости (domain functional level (DFL), forest (FFL))
  - Windows 2000 native
  - Windows Server 2003
  - Windows Server 2008
- Детальные политики паролей: AD DS Fine-Grained Password
  - Password Settings Object (PSO)
- Kerberos
  - AES 256
- Новый XML-формат, централизованное местонахождение, локализация шаблонов admx,adml
- Изменения в службах AD:
  - Active Directory Domain Services (AD DS)
  - Active Directory Lightweight Directory Services (AD LDS) – было ADAM
  - Active Directory Federation Services (AD FS) — Single Sign On, SSO
  - Active Directory Certificate Services (AD CS)
  - Active Directory Rights Management Services (AD RMS)

Ссылки

- Обзор ADFS. – (http://technet.microsoft.com/ru-ru/library/cc755828(WS.10).aspx)

- Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE: Пер. с англ. - 3-е изд., испр. — М.: Издательско-торговый дом «Русская Редакция», 2004. — 608 стр.
- “L:\Лекции\4 Курс\Администрирование в ИС\Лабораторные\02\W2K3*.pdf“
- “L:\Лекции\4 Курс\Администрирование в ИС\Лабораторные\02\DOCs\w2k3_docs\Windows.Server.2003_RUS.chm”
- http://xnets.ru/plugins/content/content.php?cat.9