

# Служба каталога Microsoft Windows Server 2003

Назначение Структура Возможности

---

# Содержание

---

- Логическая структура Active Directory и организация каталога
- Физическая структура Active Directory
- Механизмы службы каталогов для управления правами и ресурсами

# Active Directory

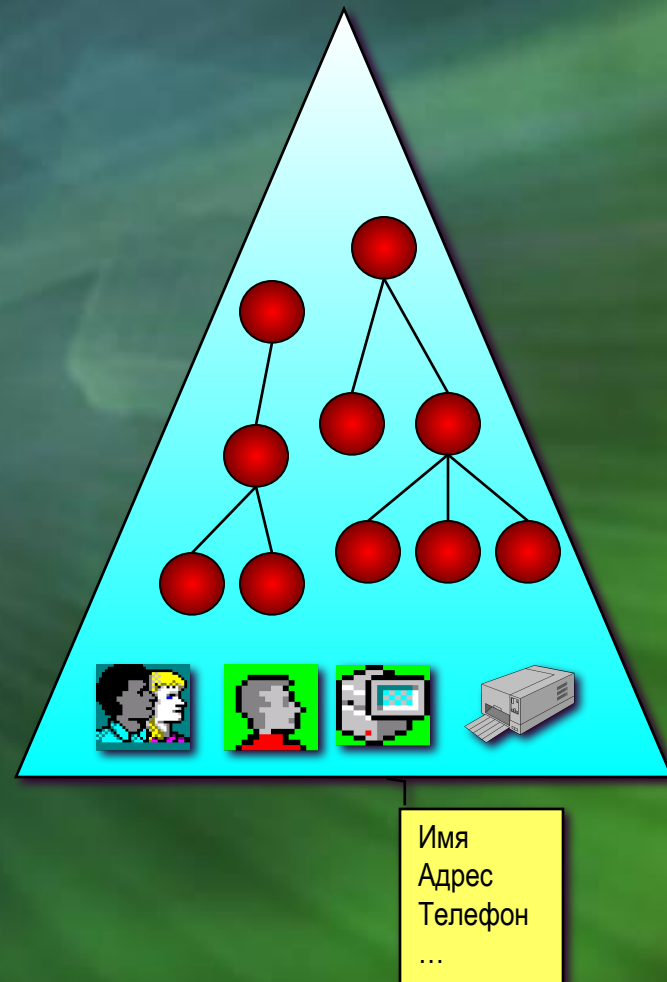
---

- Каталог
  - Глобальное распределенное хранилище информации обо всех объектах корпоративной сети
- Функции службы каталогов
  - Внедрение политики безопасности информационной системы
  - Организационное разделение каталога
  - Распределение каталога по большому количеству компьютеров в сети
  - Репликация каталога между распределенными участками

# Домен

---

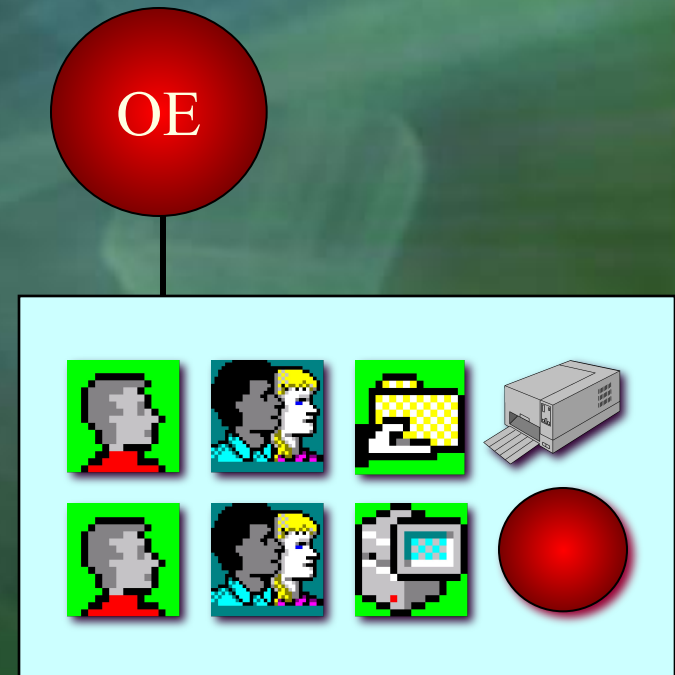
- Каталог - хранилище объектов
- Домен
  - Основная логическая единица каталога
    - Объекты
    - Объект определяется набором атрибутов
    - Организационные единицы



# Организационная единица

---

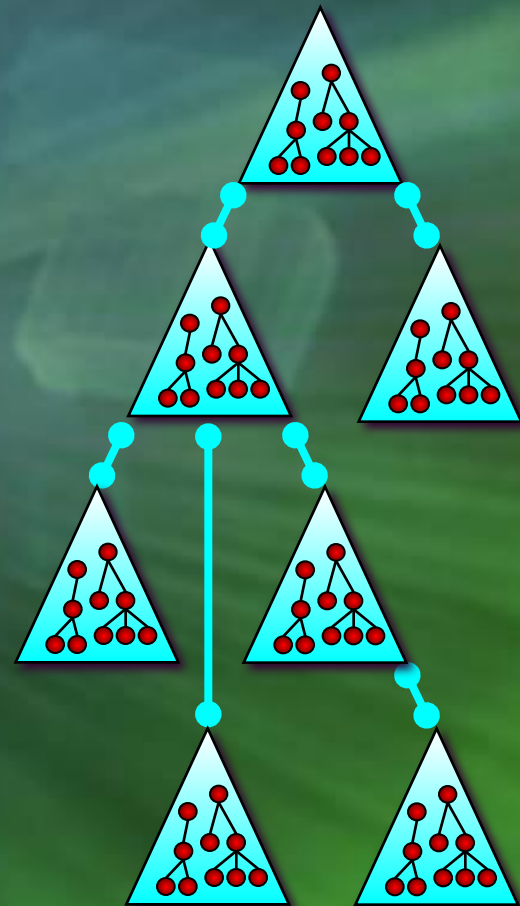
- Группировка объектов каталога внутри домена
  - Логическое упорядочение объектов домена
  - Иерархия в виде вложенных ОЕ



# Дерево

---

- Иерархическая организация доменов
  - Транзитивные отношения доверия
    - Kerberos Trust
- Единое пространство имен



# Лес (Форест)

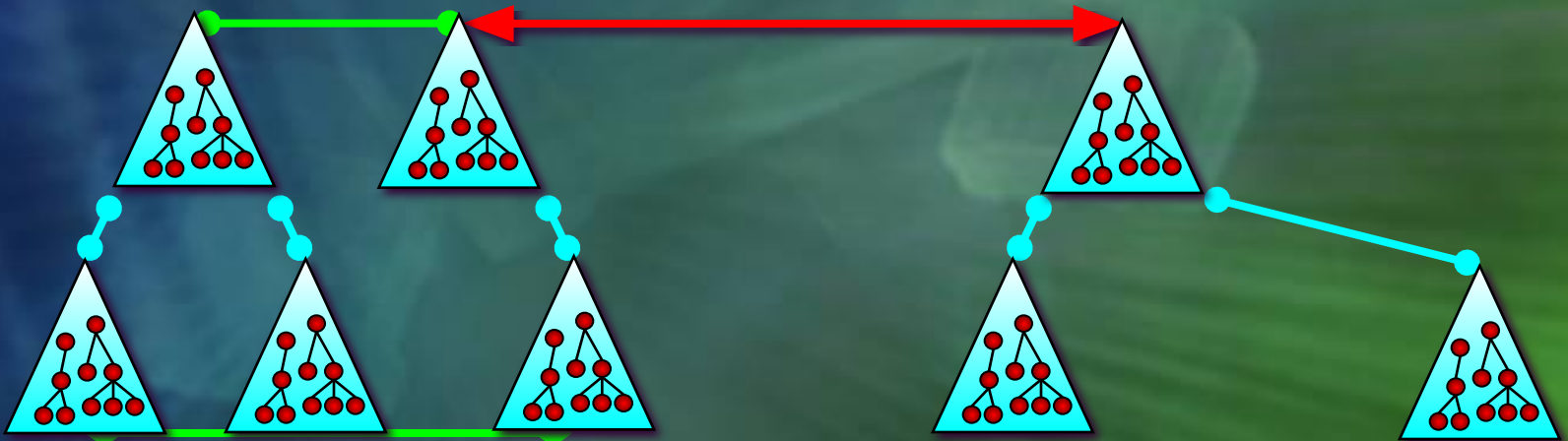
---

- Несколько деревьев, корневые домены которых связаны транзитивными отношениями доверия
  - Разные пространства имен
  - Общая Схема (Schema)
  - Общий Глобальный Каталог
- Создание леса целесообразно при построении единого каталога для нескольких организаций

# Доверительные отношения

Транзитивное доверие между  
корневыми доменами леса

Транзитивное  
доверие между  
лесами



Прямое нетранзитивное доверие  
между доменами леса

Транзитивное доверие между  
родительским и дочерним доменами



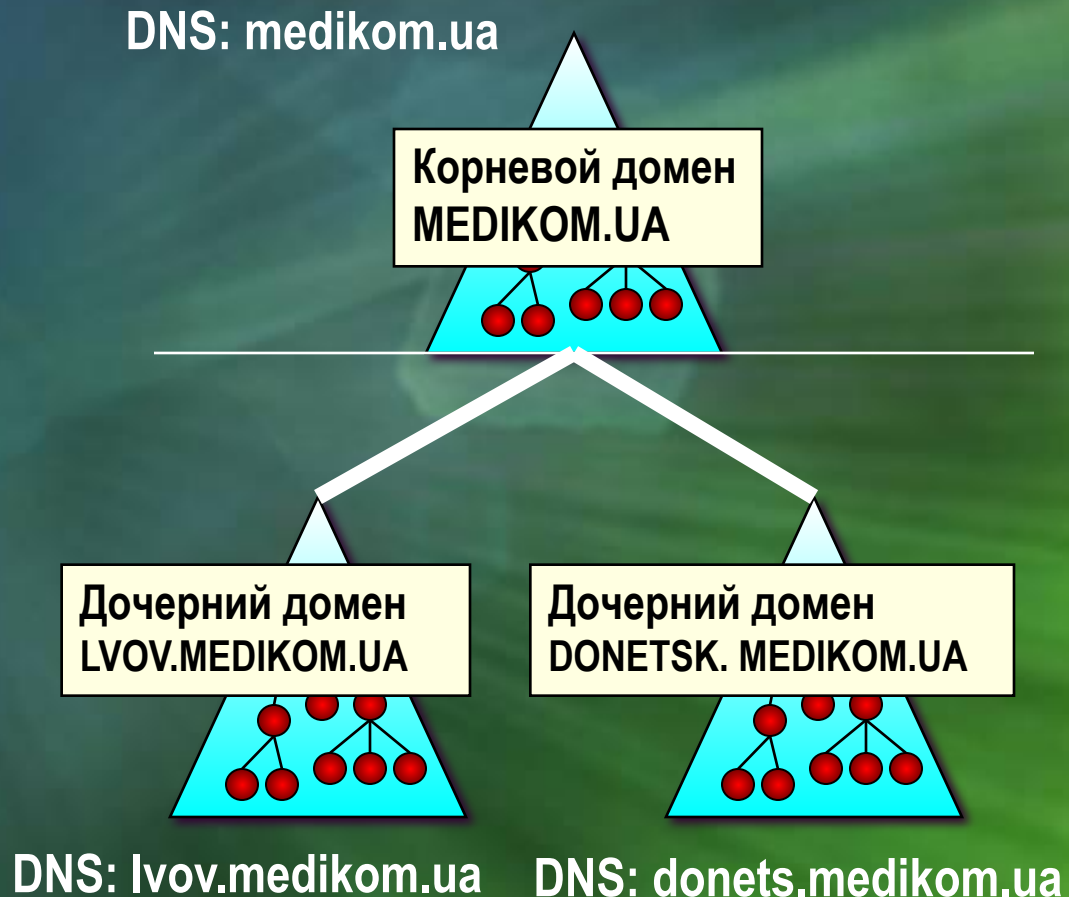
# Active Directory и DNS

---

- Каждому домену Active Directory однозначно соответствует домен DNS
  - Имена доменов Active Directory представлены в формате DNS (например `www.univ.kiev.ua`)
- Клиенты используют сервер DNS для обнаружения служб Active Directory
  - Специальные требования к серверу DNS
    - Service Resource Records (`SRV RR`)
    - Динамическое обновление базы
    - Инкрементный перенос зоны (`BIND 8.2.0 or later`)
  - Инструменты для диагностики и отладки сервера DNS (`nslookup`)

# Пространство имен

- Иерархия DNS-имен доменов отражает структуру дерева/леса
- Домен можно переименовать
  - Утилита `Rendom.exe`



# Схема

---

- Описание классов и атрибутов объектов, определенных в каталоге
  - Единая для всего каталога
- Необходимость в модификации схемы возникает крайне редко
  - Внесение специфического атрибута, не описанного в стандартной схеме
  - Установка приложений, которые вносят изменения в схему
    - Microsoft Exchange Server,
    - Microsoft ISA Server

# Модификация схемы

---

- Права на модификацию схемы есть только у специальной группы
  - **Schema Admins**
- Инструменты
  - *Active Directory Schema (mmc snap-in)*
  - Исполняемый сценарий (ADSI)

# Содержание

---

- Логическая структура Active Directory и организация каталога
- Физическая структура Active Directory
- Механизмы службы каталогов для управления правами и ресурсами

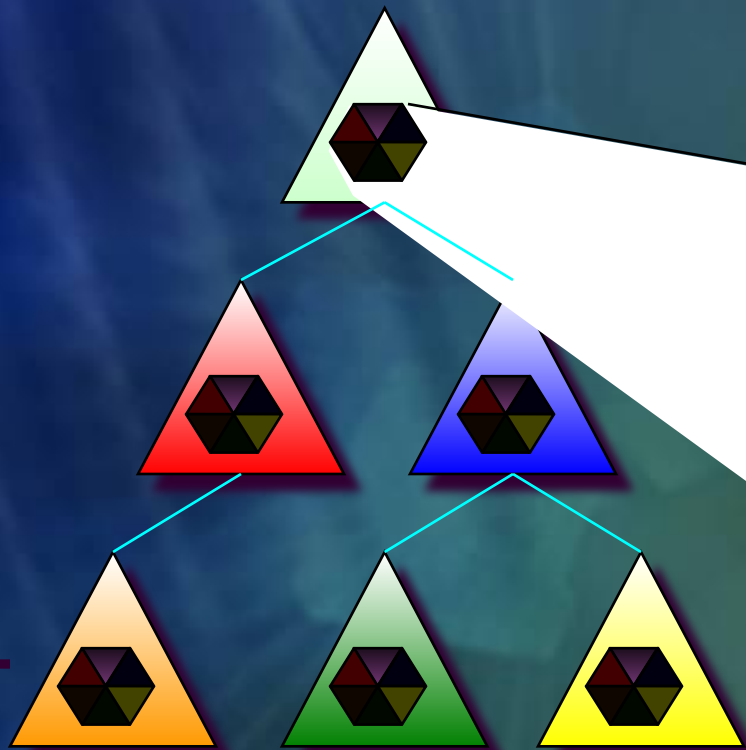
# Структура каталога

---

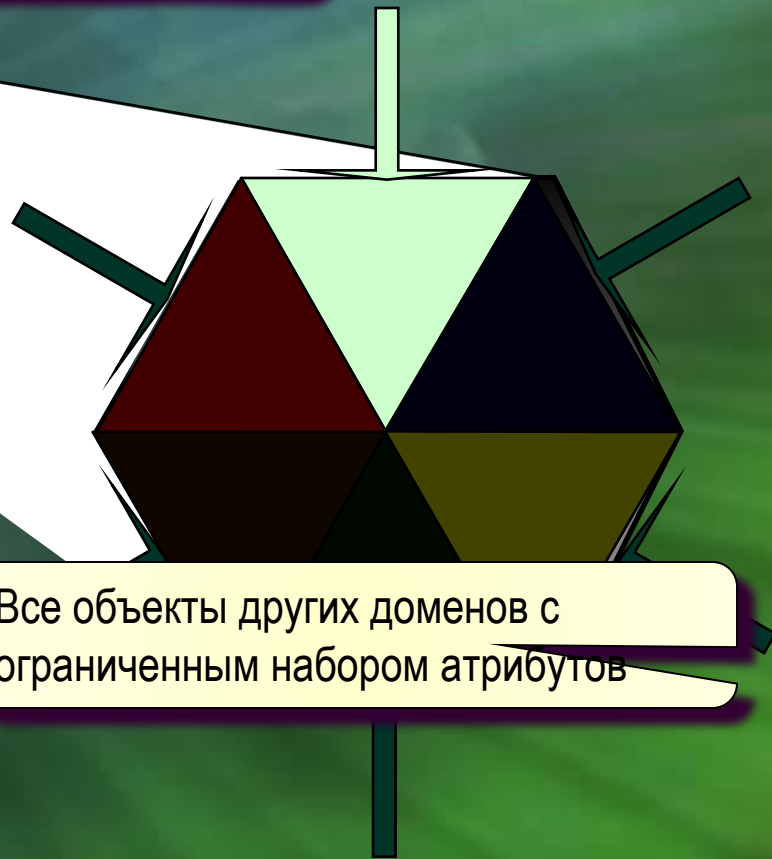
- Распределенная база данных
  - База данных объектов домена
    - Собственная для каждого домена
    - Хранится в одинаковых копиях на всех контроллерах одного домена
  - Глобальная информация дерева
    - Конфигурация каталога
    - Схема
- Глобальный каталог
  - Частичная информация обо всех объектах дерева
  - В каждом домене присутствует хотя бы один сервер Глобального каталога

# Глобальный каталог

Ссылка на базу данных  
собственного домена



Все объекты других доменов с  
ограниченным набором атрибутов



# Компоненты каталога





# Контроллер домена

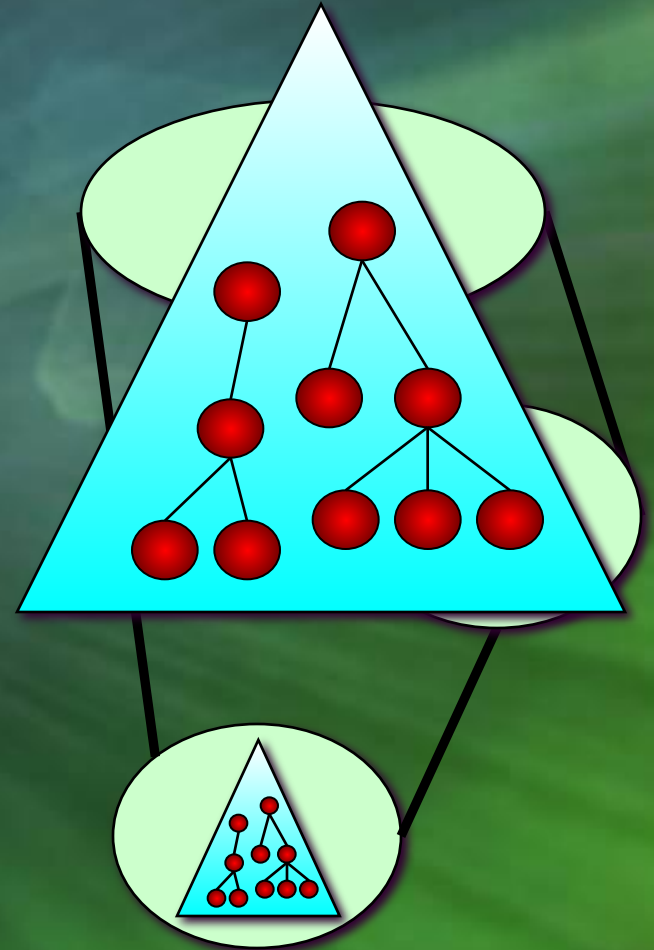
---

- Windows Server 2003 с установленной службой Active Directory
- Хранит копию базы данных объектов домена и участвует в репликации с другими контроллерами домена
- Выполняет аутентификацию и авторизацию пользователей и компьютеров
- Обеспечивают отказоустойчивую работу предприятия



# Сайт

- Сайт
  - Группа компьютеров, связанных между собой "быстрыми" линиями
  - Структура сайтов отражает топологию сетевых коммуникаций



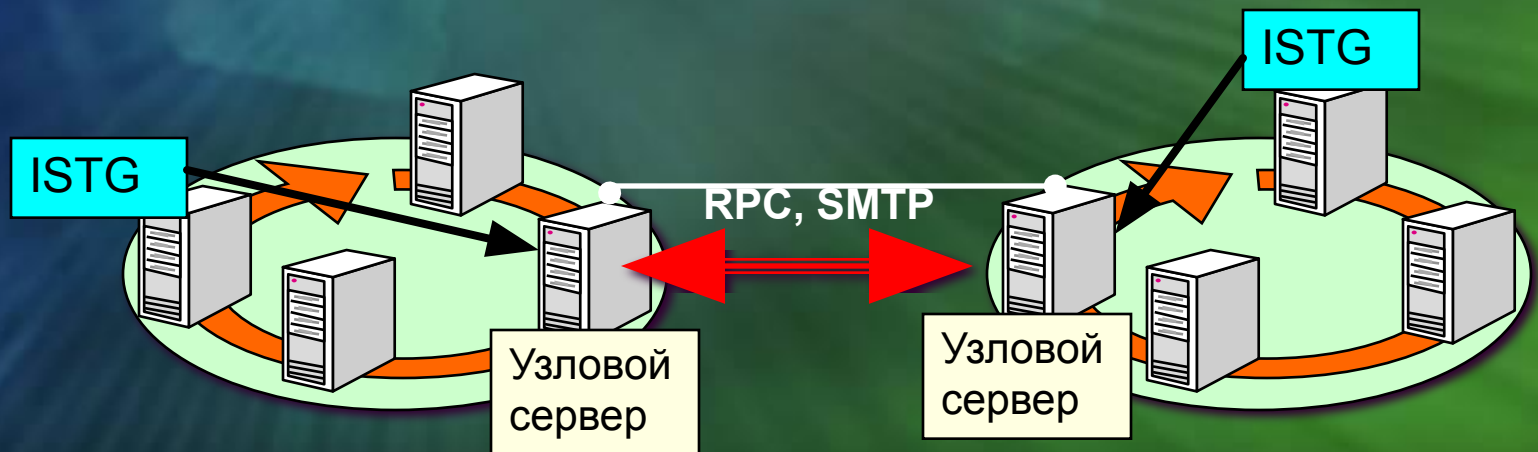
# Репликация каталога

---

- Принцип «Multi-master»
  - Все контроллеры равноправны
  - Все реплики разделов каталога доступны для записи
- Синхронизация реплик каталога, хранящихся на разных контроллерах
  - Update Sequence Number (USN)
  - Разрешение конфликтов
- Детализация до уровня отдельного атрибута
  - Реплицируются только отдельные атрибуты

# Топология репликации

- Knowledge Consistency Checker (KCC)
  - Организует репликацию внутри сайтов
- Inter-Site Topology Generator (ISTG)
  - Автоматически формирует топологию репликации и между сайтами
- Узловой сервер сайта
  - Выполняет репликацию через соединение с узловым сервером сайта-партнера



# Серверы FSMO

---

- Flexible Single-Master Operations
  - Операции, которые нельзя одновременно выполнять на нескольких машинах
- Пять ролей FSMO
  - Единственный сервер на лес
    - Schema Master
    - Domain Naming Master
  - Один сервер в каждом домене
    - Relative Identifier (RID) Master
    - Primary Domain Controller (PDC) Emulator
    - Infrastructure Master

# Содержание

---

- Компоненты Active Directory и организация каталога
- Физическая структура Active Directory
- Механизмы службы каталога для управления правами и ресурсами

# Основные операции

---

- Управление объектами каталога
- Публикация ресурсов и служб
- Организация поиска в каталоге
- Интеграция с системой безопасности Windows 2003
  - Аутентификация
  - Службы сертификатов
  - Контроль доступа к объектам (ACL)
- Управление конфигурациями рабочих станций пользователей

# Делегирование

---

- Административные полномочия, которые можно делегировать пользователям или группам
  - Изменение свойств контейнера
  - Создание, модификация и удаление дочерних объектов
  - Изменение указанных атрибутов у объектов определенного класса
  - Создание новых пользователей и групп
  - Управление пользователями и группами в рамках контейнера
  - Управление групповыми политиками



# Делегирование прав

---

- Управление объектами
  - Административные или специальные права на домен или организационную единицу
- Выполнение задач
  - Права на выполнение конкретной операции с указанными объектами
- Редактирование свойств
  - Права на изменение конкретных указанных параметров объекта

# Средства выполнения делегированных задач

Users - [Users]

## Звери нашего зоопарка

Name	Full Name	Description
ACTUser	Application Center Test A...	Account used to launch the Applicati...
adolf	adolf	
ASPNET	ASP.NET Machine Account	Account used for running the ASP.N...
delf	delf	
dima	dima	
eddy	eddy	
ftp-user		
Guest		Built-in account for guest access to t...
IUSR_BILLY-GW	Internet Guest Account	Built-in account for anonymous acce...
IWAM_BILLY-...	Launch IIS Process Account	Built-in account for Internet Informa...
kka	kka	
mumia	mumia	
nau	nau	
nina	nina	
raol	raol	
rebel	rebel	rebel
root		Built-in account for administering the...
root-2	root-2	
schkiel	schkiel	
SQLDebugger	SQLDebugger	This user account is used by the Visu...
squash	squash	



Свойство  
зверя



Переимено...



Угробить



Сменить  
пароль...



Новенький...

# Групповая политика

---

- Централизованное управления свойствами компьютеров и рабочей среды пользователей Windows 2000/XP
  - Параметры безопасности
  - Свойства рабочего стола пользователя
  - Сценарии входа/выхода пользователей, загрузки/выключения компьютеров
  - Управление членством в группах
  - Параметры работы операционной системы клиентов (службы, программы)
  - Автоматическая установка, обновление и удаление ПО

# Параметры групповых политик

---

- Большинство параметров имеют три значения



- 2 ветви конфигураций

- Настройки компьютера переписывают настройки пользователя



- Для получения GPO учетная запись (компьютера или пользователя) :

- Должна находиться в ОЕ, которой назначена политика
- Должна иметь разрешение "Read and Apply Group Policy"

# Уровни применения ГП

---

- Сайт
  - Все домены внутри сайта
- Домен
  - Все пользователи и компьютеры домена
  - ГП не наследуется дочерними доменами
- Организационная единица
  - Все пользователи и компьютеры ОЕ
  - ГП применяется ко всем вложенным ОЕ

# Порядок применения

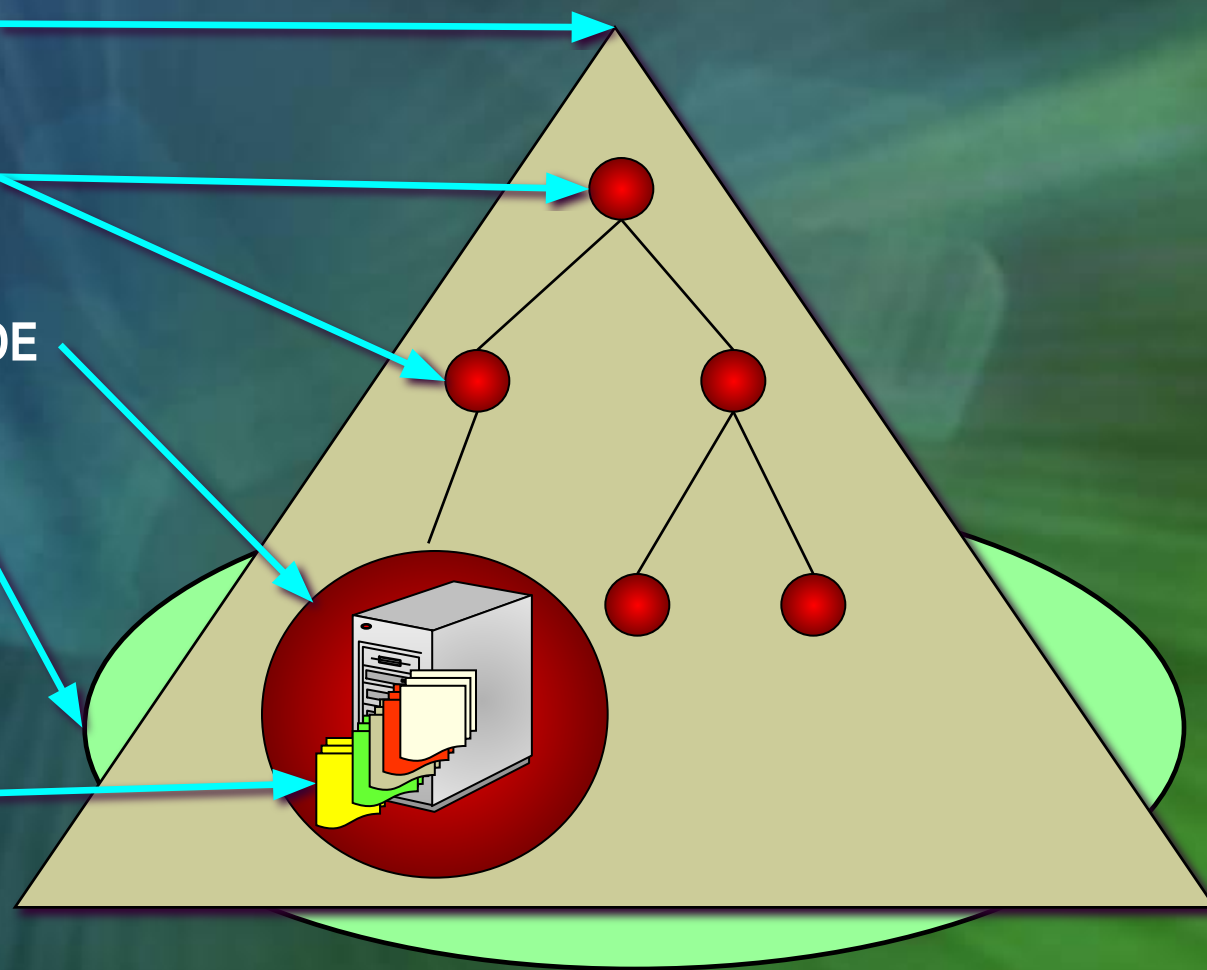
Политика домена

Политики  
родительских ОЕ

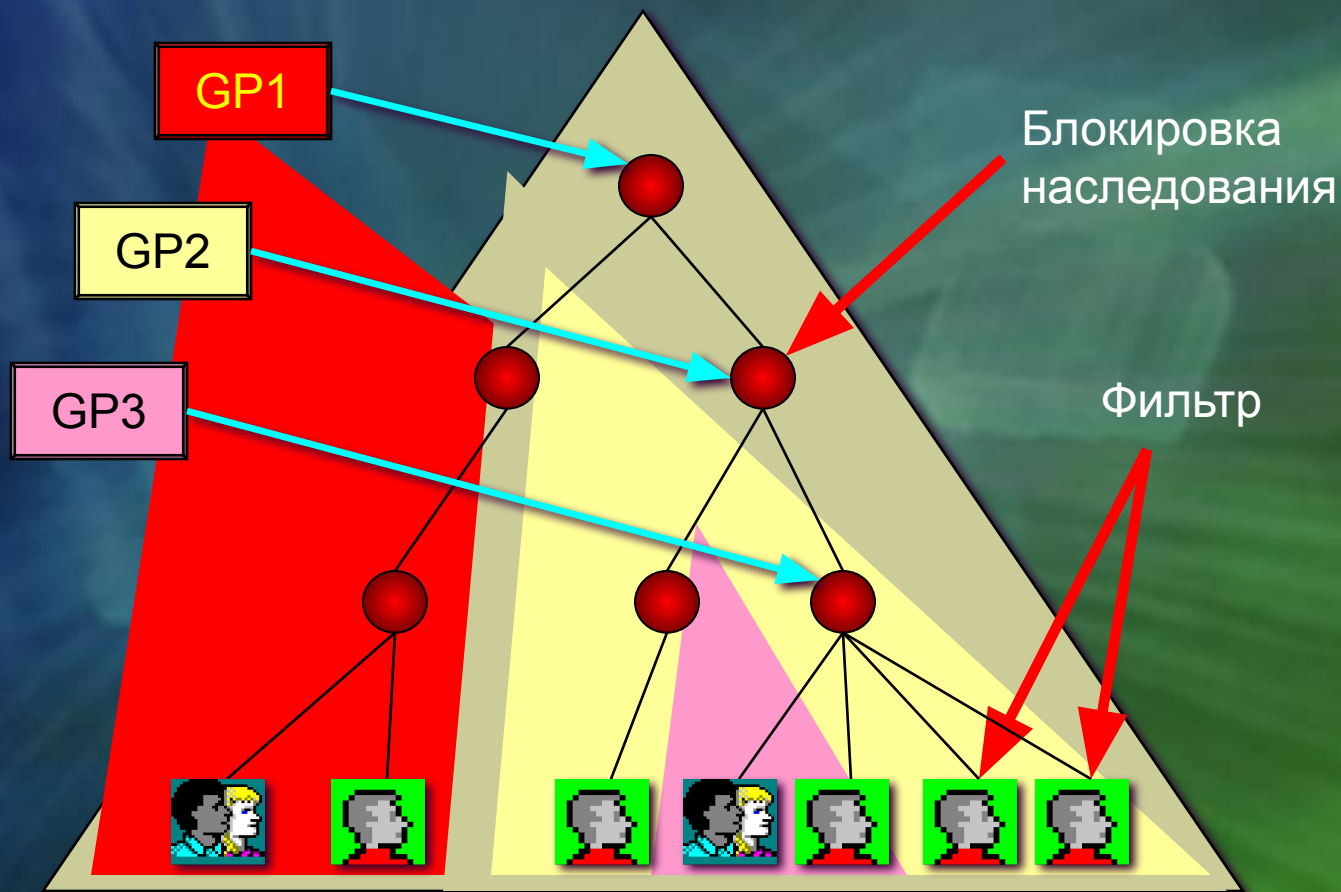
Политика своего ОЕ

Политика сайта

Локальная политика



# Наследование ГП



# Фильтры WMI

---

- Новый механизм, позволяющий фильтровать объекты, к которым применяется групповая политика
  - Новый тип объекта в Active Directory
  - Работает только для машин Windows XP Professional и Windows 2003
- Объекту групповой политики может соответствовать один фильтр WMI
- Фильтр WMI может быть назначен нескольким объектам GPO



# Group Policy Management Console

---

- Объединенная консоль для управления групповыми политиками
  - Консолидирует все операции управления GPO из разных инструментов
  - Организует данные групповых политик
  - Визуально показывает связи объектов GPO и контейнеров



# Анализ результатов применения

- Раздел "Results" в консоли GPMC
- Работает на машинах Windows XP и Windows 2003
- Необходимо подключение к анализируемому компьютеру
- Необходима регистрация пользователя

administrator on DEMO2003

Summary Settings Policy Events

### Group Policy Results

DEMO\administrator on DEMO\DEMO2003  
Data collected on: 11.06.2003 12:11:34 [show all](#)

**Summary** [hide](#)

**Computer Configuration Summary** [hide](#)

**General** [show](#)

**Group Policy Objects** [hide](#)

**Applied GPOs** [show](#)

**Denied GPOs** [hide](#)

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty
GP with WMI Filter	Demo.MS	False WMI Filter

**Security Group Membership when Group Policy was applied** [show](#)

**WMI Filters** [show](#)

**Component Status** [show](#)

**User Configuration Summary** [hide](#)

**General** [show](#)

**Group Policy Objects** [show](#)

**Security Group Membership when Group Policy was applied** [hide](#)

DEMO\Domain Users  
Everyone  
BUII.TIN\Administrators

# Моделирование результатов

---

- Симуляция процесса применения групповых политик
  - Раздел “Modeling” в консоли GPMC
- Позволяет рассматривать множество гипотетических вариантов
  - Членство в группах, местоположение объектов, фильтры WMI и др.

# Курсы Microsoft Official Curriculum (MOC)

---

- 2274 Managing a Windows Server 2003 Environment
- 2279 Planning, Implementing and Maintaining a Windows Server 2003 Active Directory Infrastructure

# Вопросы

---