Служба каталога Microsoft Windows Server 2003

Назначение Структура Возможности

Содержание

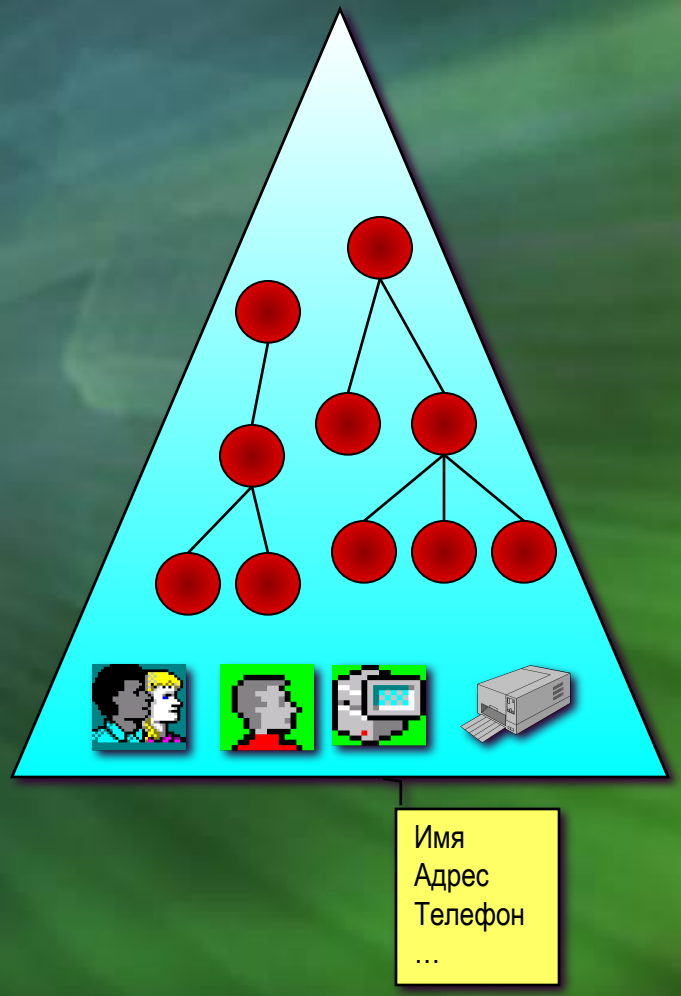
- Логическая структура Active Directory и организация каталога
- Физическая структура Active Directory
- Механизмы службы каталогов для управления правами и ресурсами

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

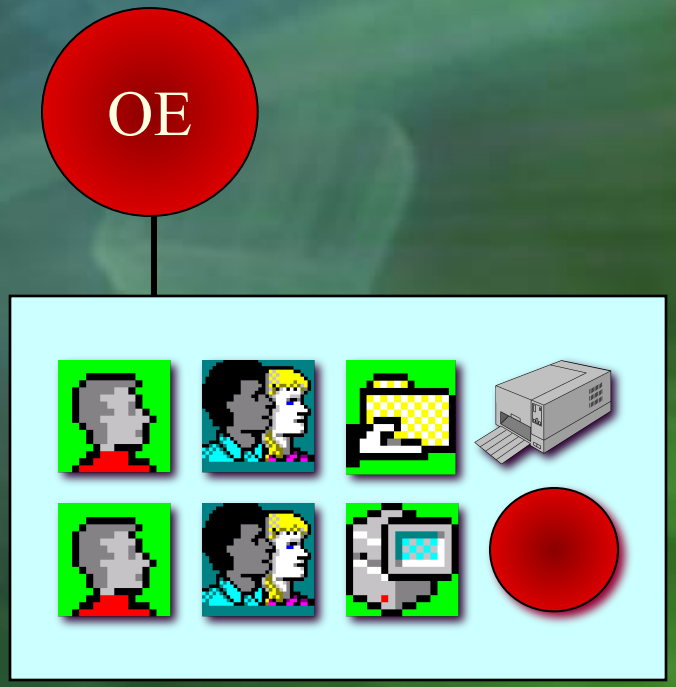
Домен

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



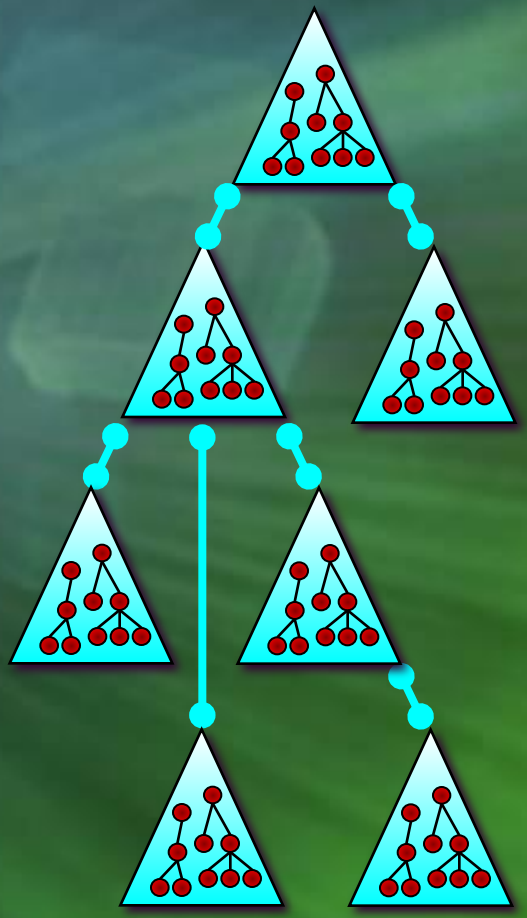
Организационная единица

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



Дерево

- Иерархическая организация доменов
  - Транзитивные отношения доверия
  - Направленность
- Единое пространство имен



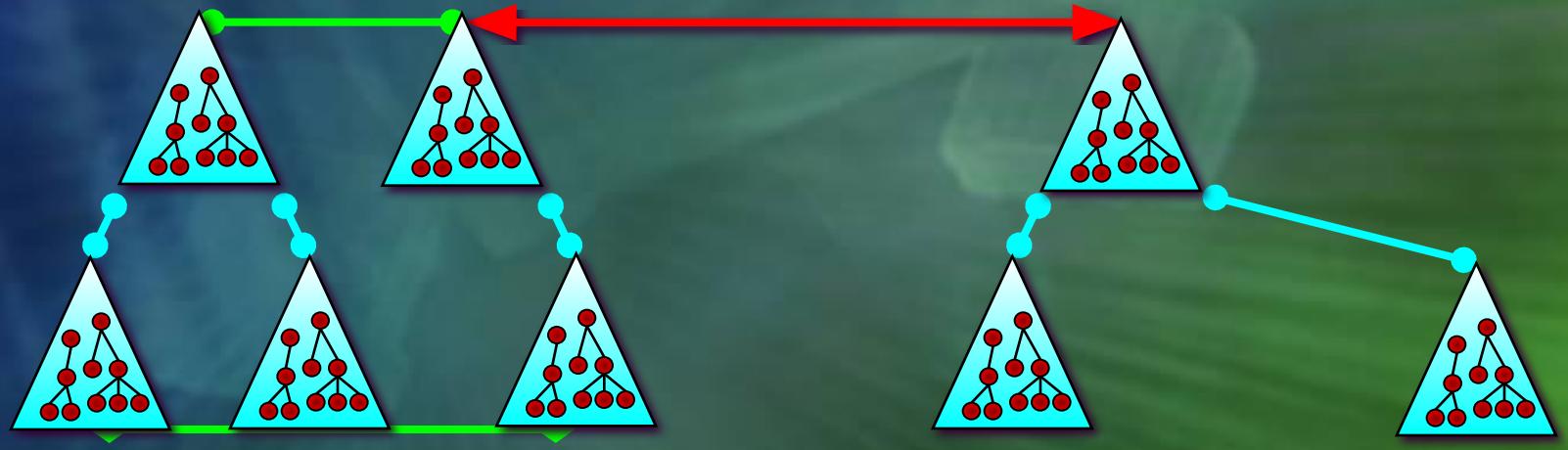
Лес (Форест)

- 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

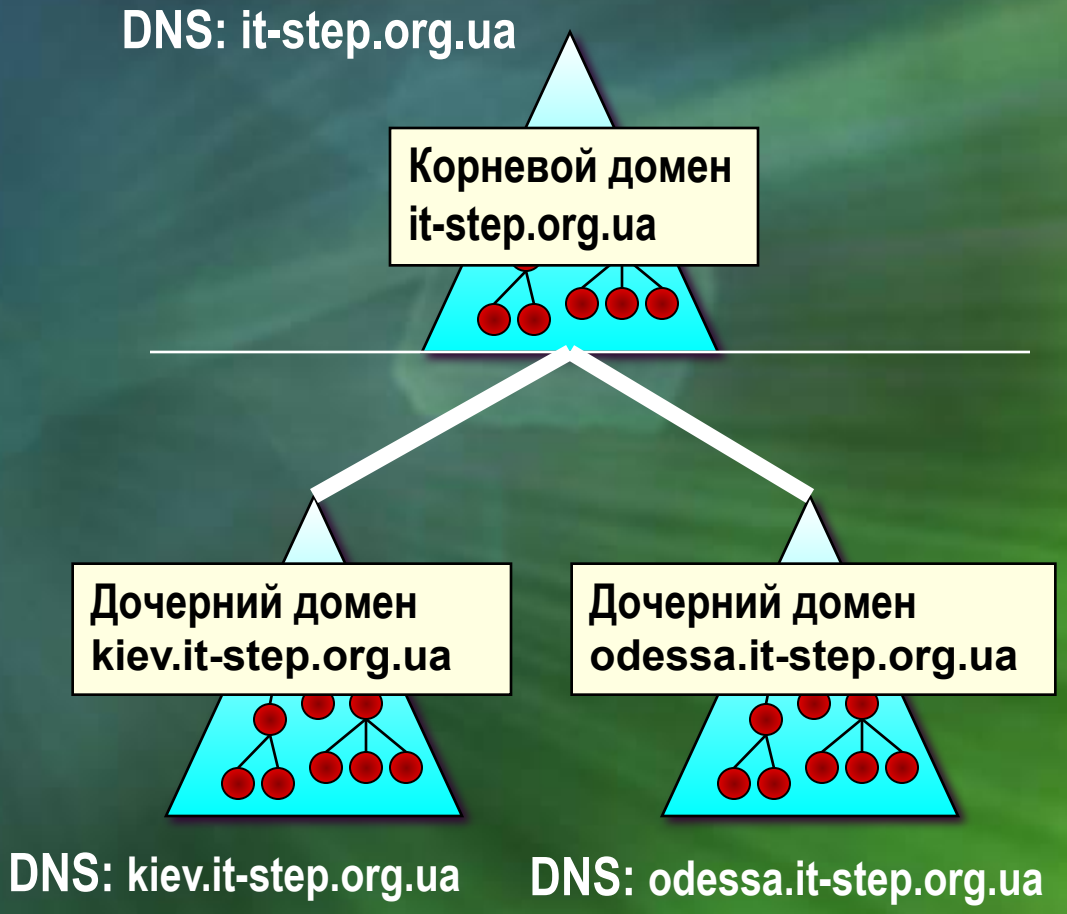
Транзитивное доверие между родительским и дочерним доменами

Active Directory и DNS

- Каждому домену Active Directory однозначно соответствует домен DNS
  - Имена доменов Active Directory представлены в формате DNS (например it-step.org.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)*

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

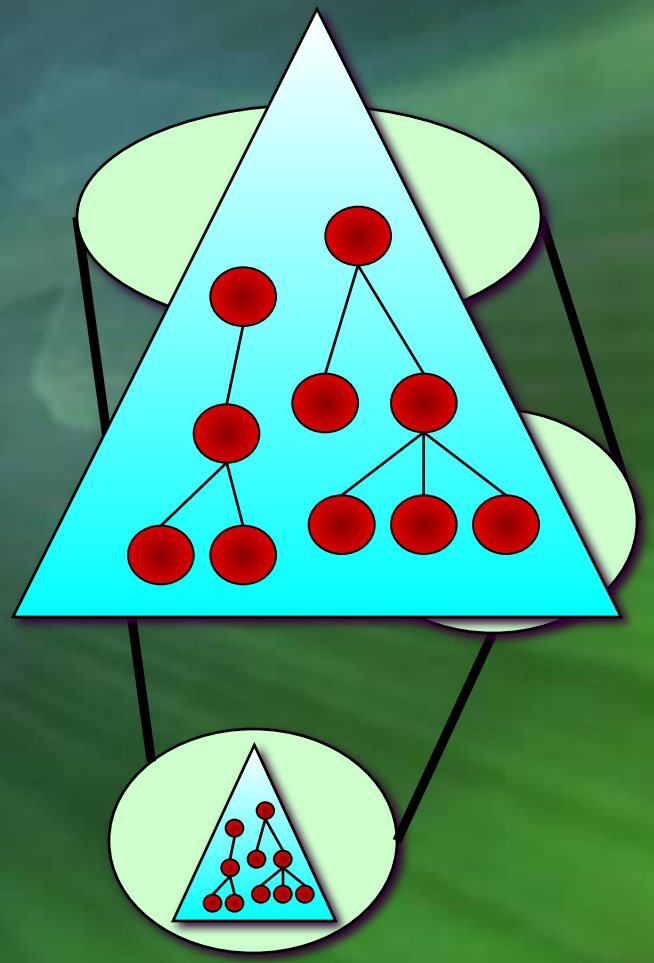
Компоненты каталога

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

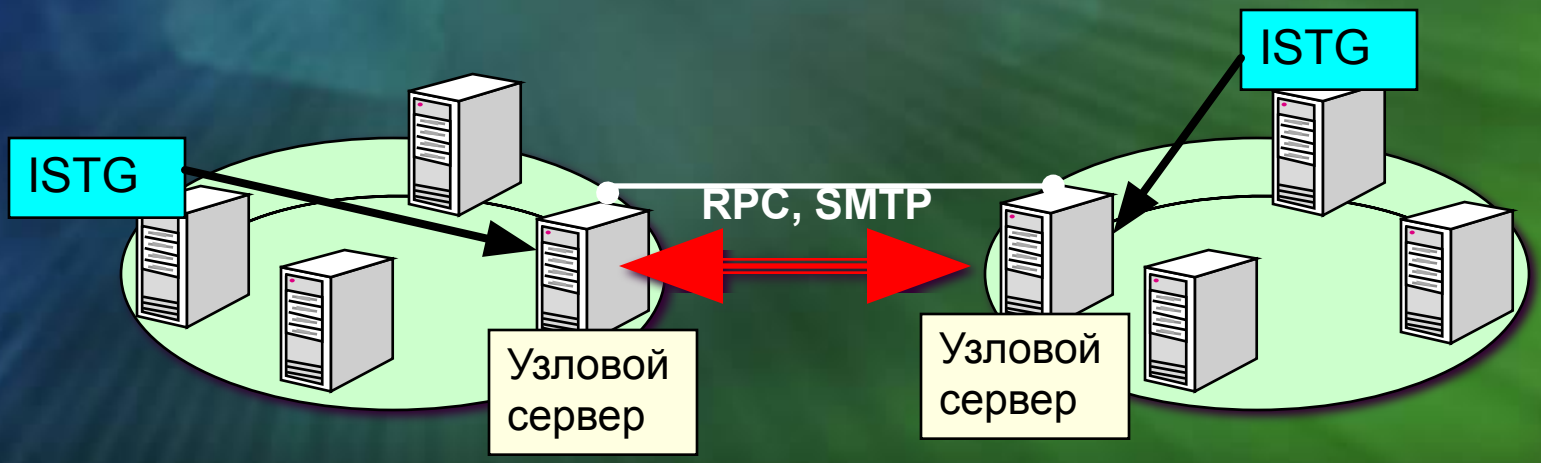


Репликация каталога

- Принцип «Multi-master»
  - Все контроллеры равноправны
  - Все реплики разделов каталога доступны для записи
- Синхронизация реплик каталога, хранящихся на разных контроллерах
- 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

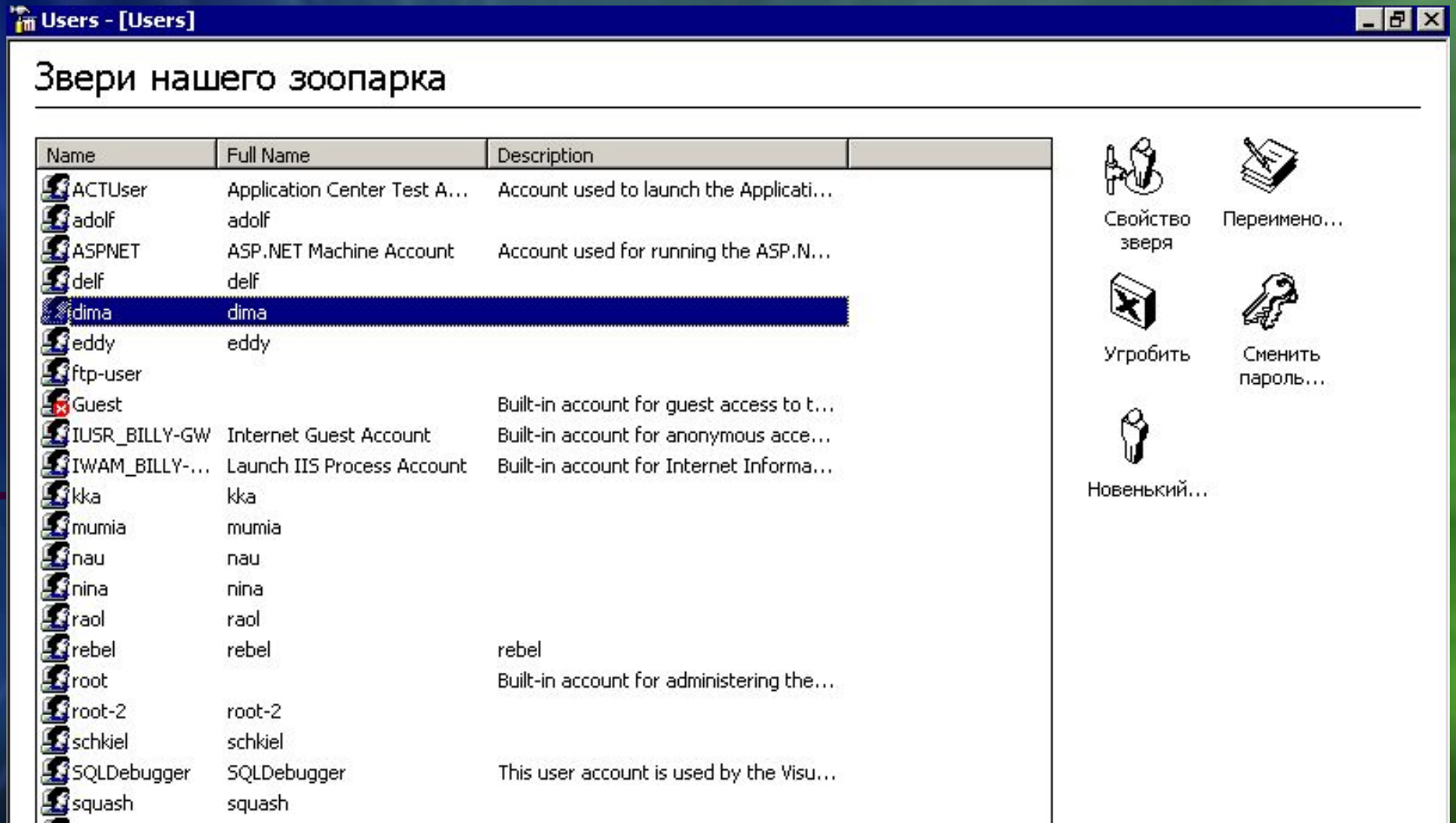
Делегирование

- 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

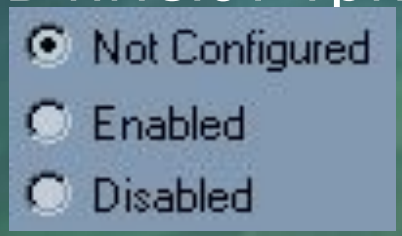


Групповая политика

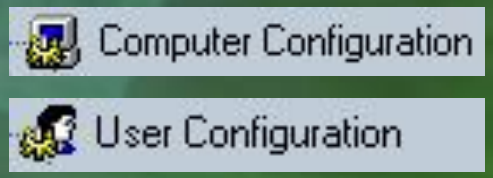
- Централизированное управления свойствами компьютеров и рабочей среды пользователей Windows 2000/XP
  - Параметры безопасности
  - Свойства рабочего стола пользователя
  - Сценарии входа/выхода пользователей, загрузки/выключения компьютеров
  - Управление членством в группах
  - Параметры работы операционной 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

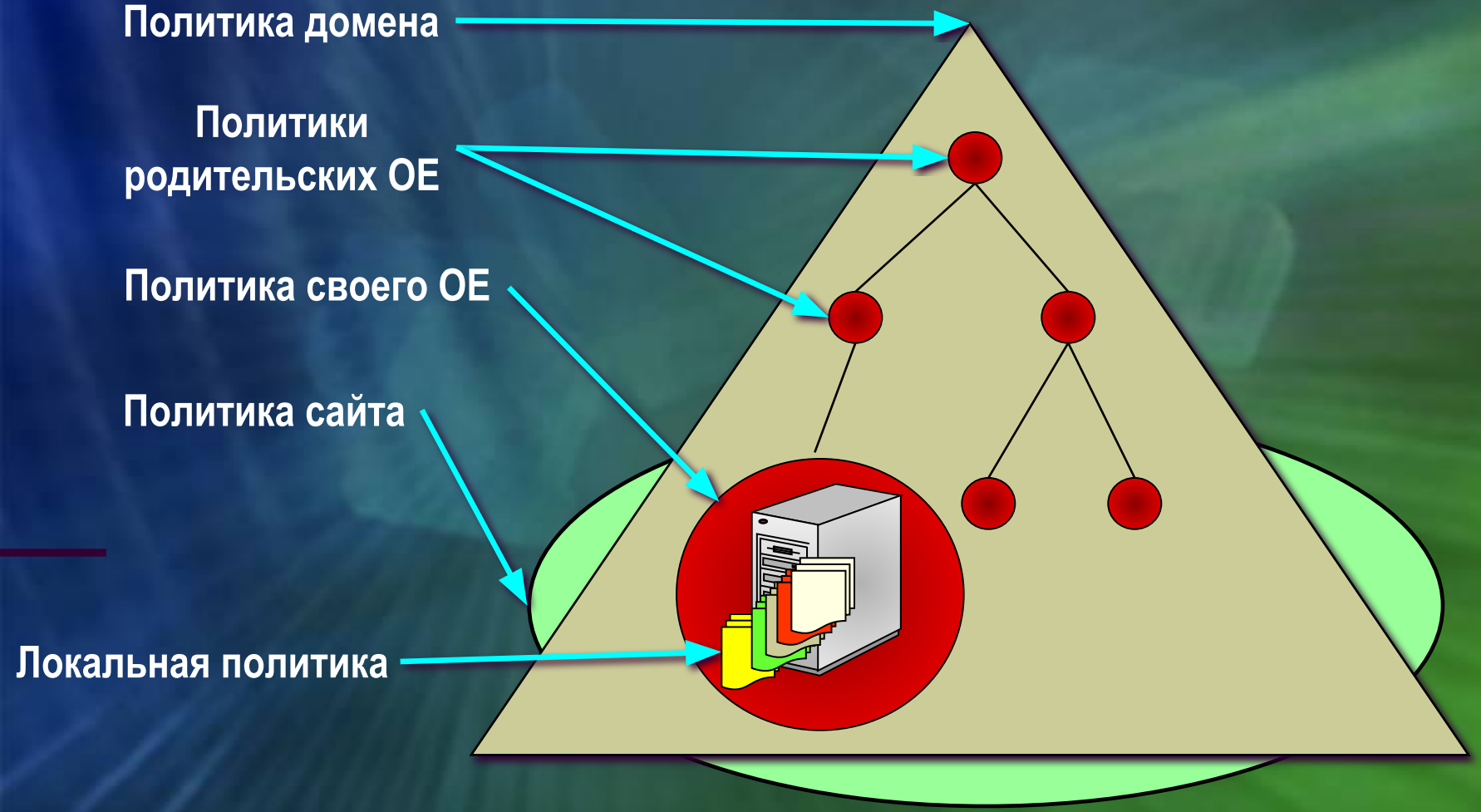


- Для получения GPO учетная запись (компьютера или пользователя) :
  - Должна находиться в OE, которой назначена политика
  - Должна иметь разрешение “Read and Apply Group Policy”

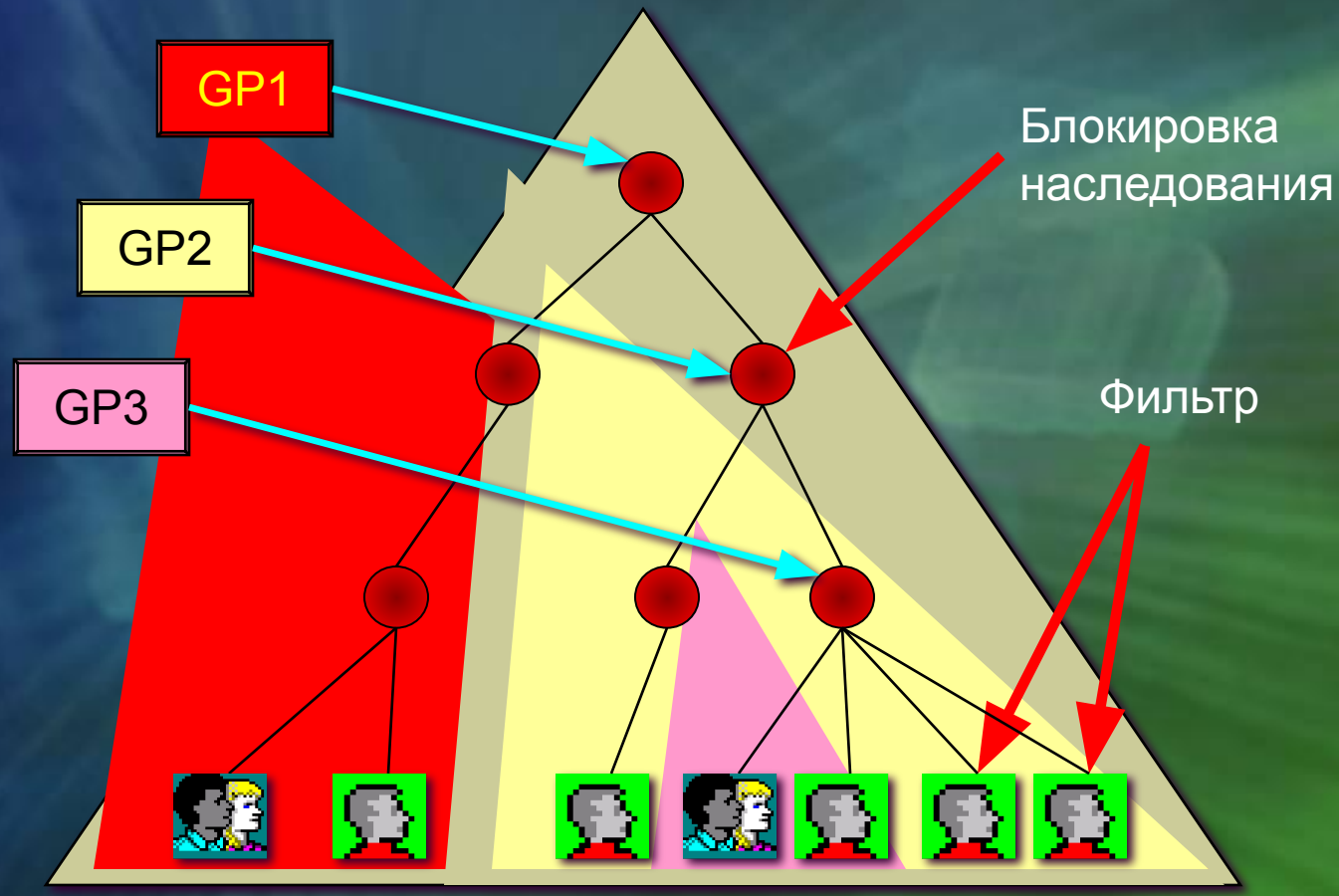
Уровни применения ГП

- 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



Наследование ГП



Group Policy Management Console

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