Служба каталогов

- Directory Service (служба каталогов) – это составное понятие, означающее как собственно хранилище данных, так и службы, обеспечивающие доступ к хранимой информации со стороны пользователей и приложений
- В настоящее время наиболее распространенными реализациями службы Directory Services являются:
  - Novell, eDirectory (ранее Novell DS, NDS)
  - Sun, Java System Directory Server
  - Microsoft, Active Directory

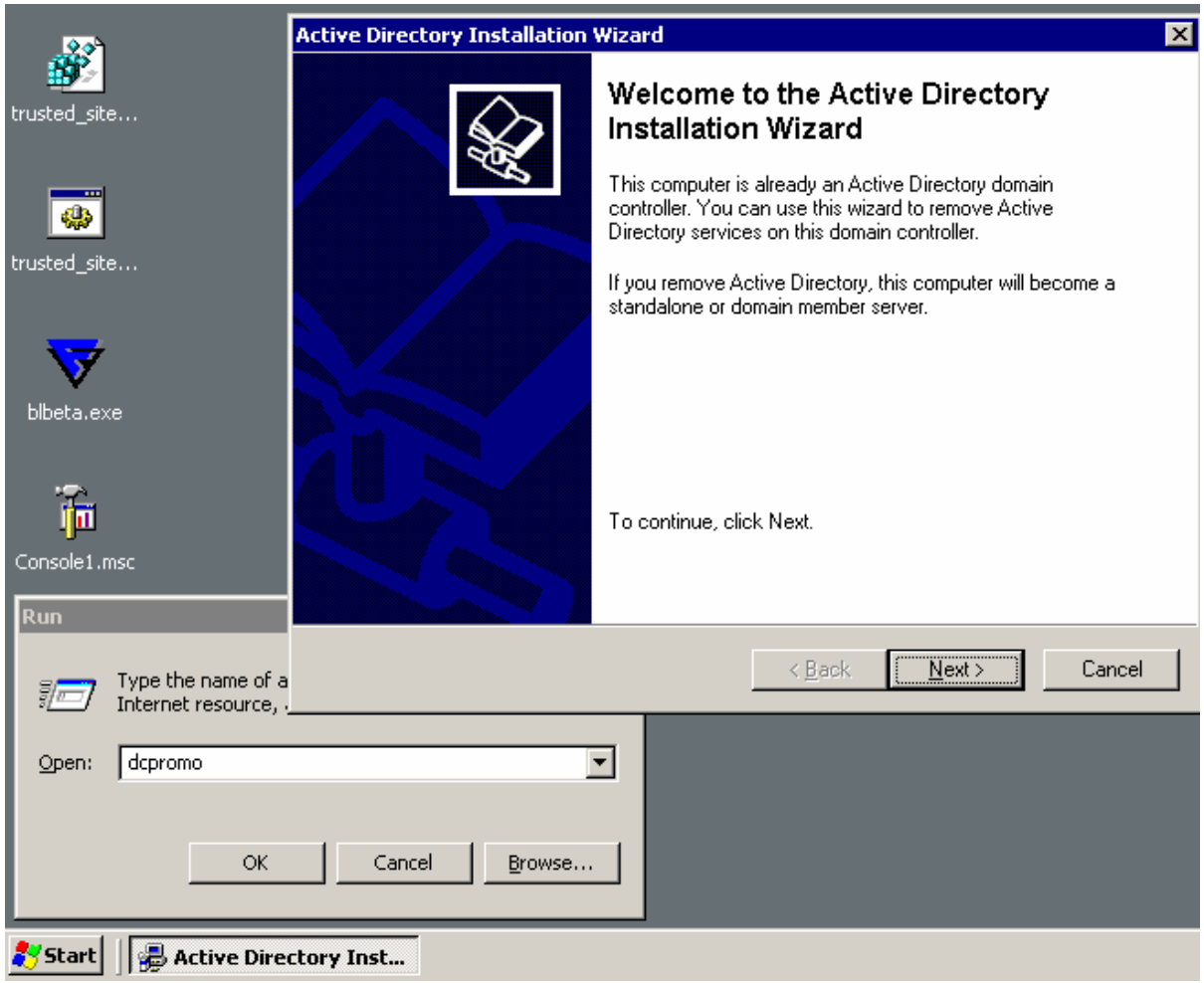
Служба каталогов Active Directory

- Базируется на спецификации службы распределенного каталога X.500, протоколе доступа к службе каталога LDAP и службе DNS
- Логическая структура
  - Три основных структурных уровня: домены, деревья доменов и леса
  - Подразделения (OU, Organizational Units)
  - Глобальные каталоги (GC, Global Catalogs), содержащие данные о часто используемых объектах AD (read-only реплицируемые копии) в пределах леса доменов.
- Физическая структура
  - контроллеры домена (DC, Domain Controllers)
  - сайты (sites)

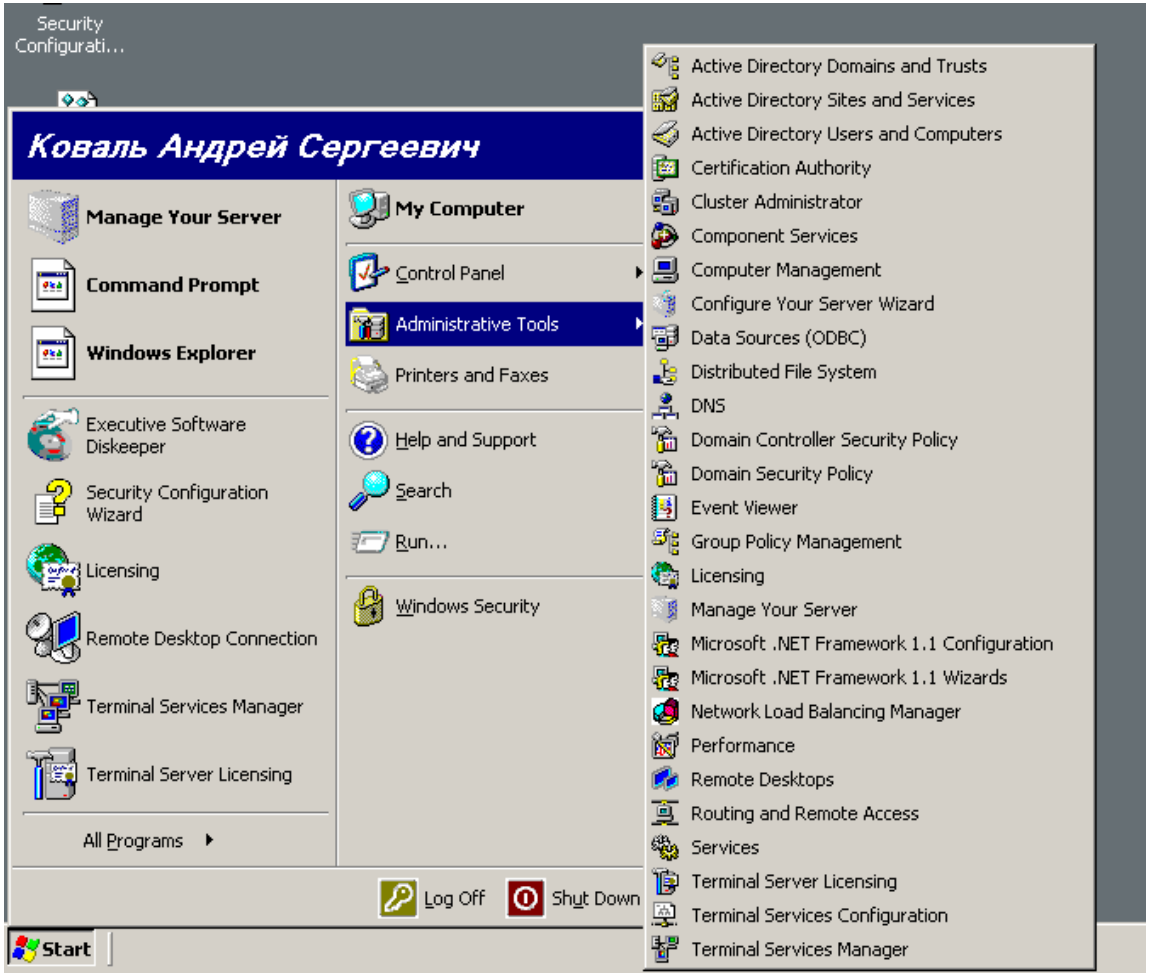
Имена LDAP протокола

- Два типа имен
  - Различаемые имена (DN, Distiguished Names)
  - Относительные различаемые имена RDN
  - Пример DN
    - CN=ivanov,OU=Люди,DC=cs,DC=vsu,DC=ru
  - Элементы DN
    - обычное имя (CN, Common Name)
    - подразделение, организационная единица (OU, Organizational Unit)
    - часть DNS-имени (DC, Domain Component)

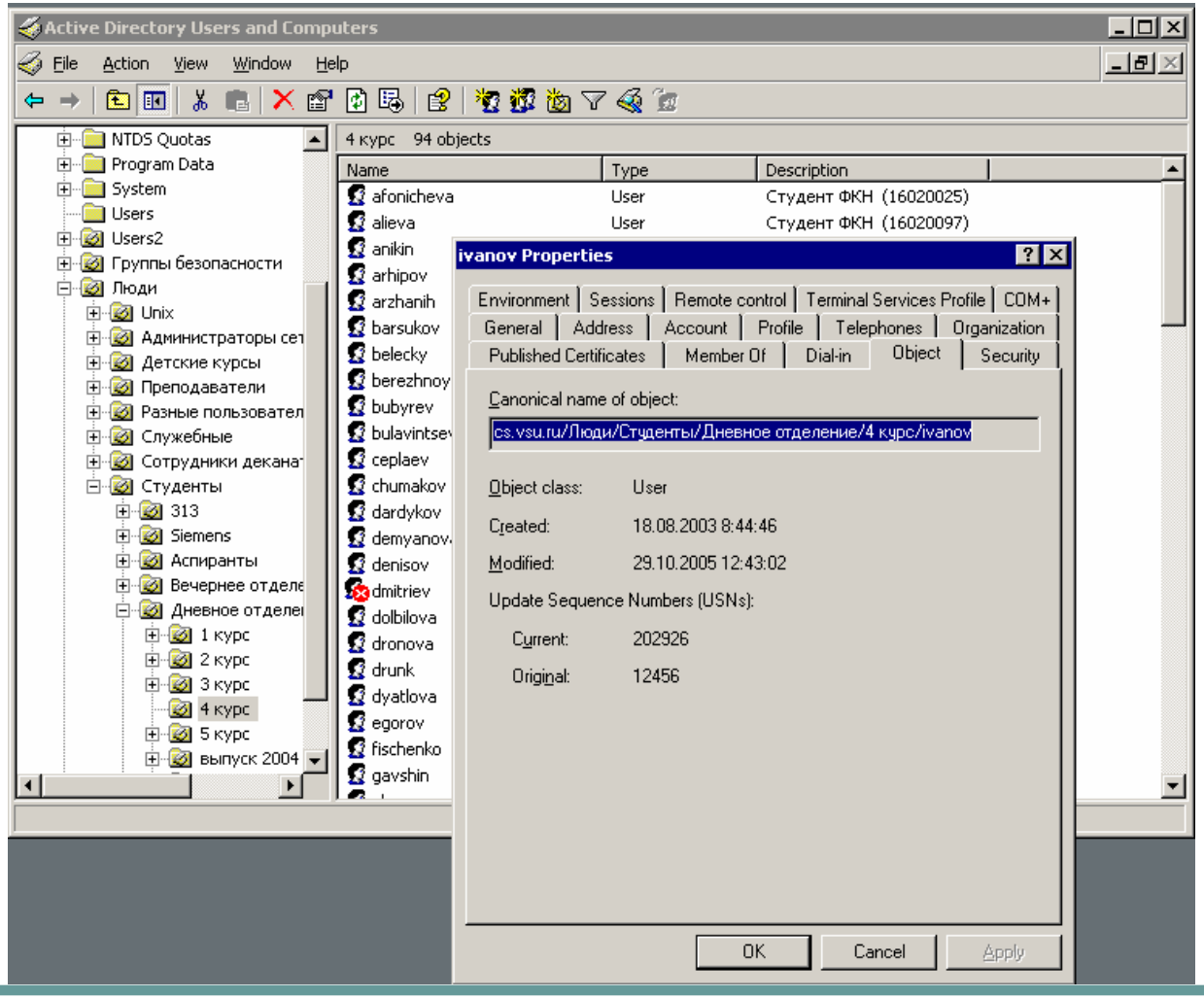
Мастер установки Active Directory



Консоли управления AD



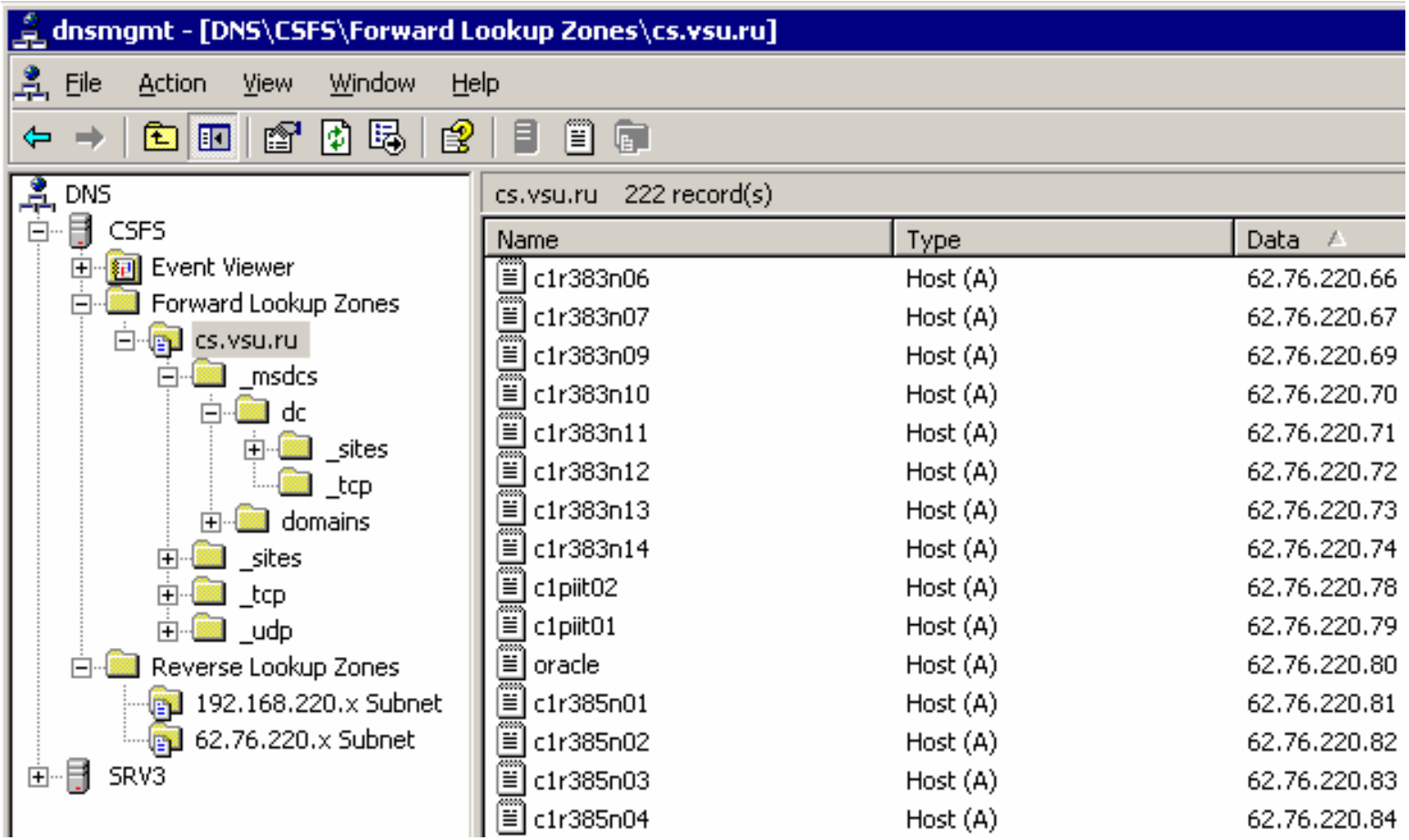
Объект AD в консоли управления



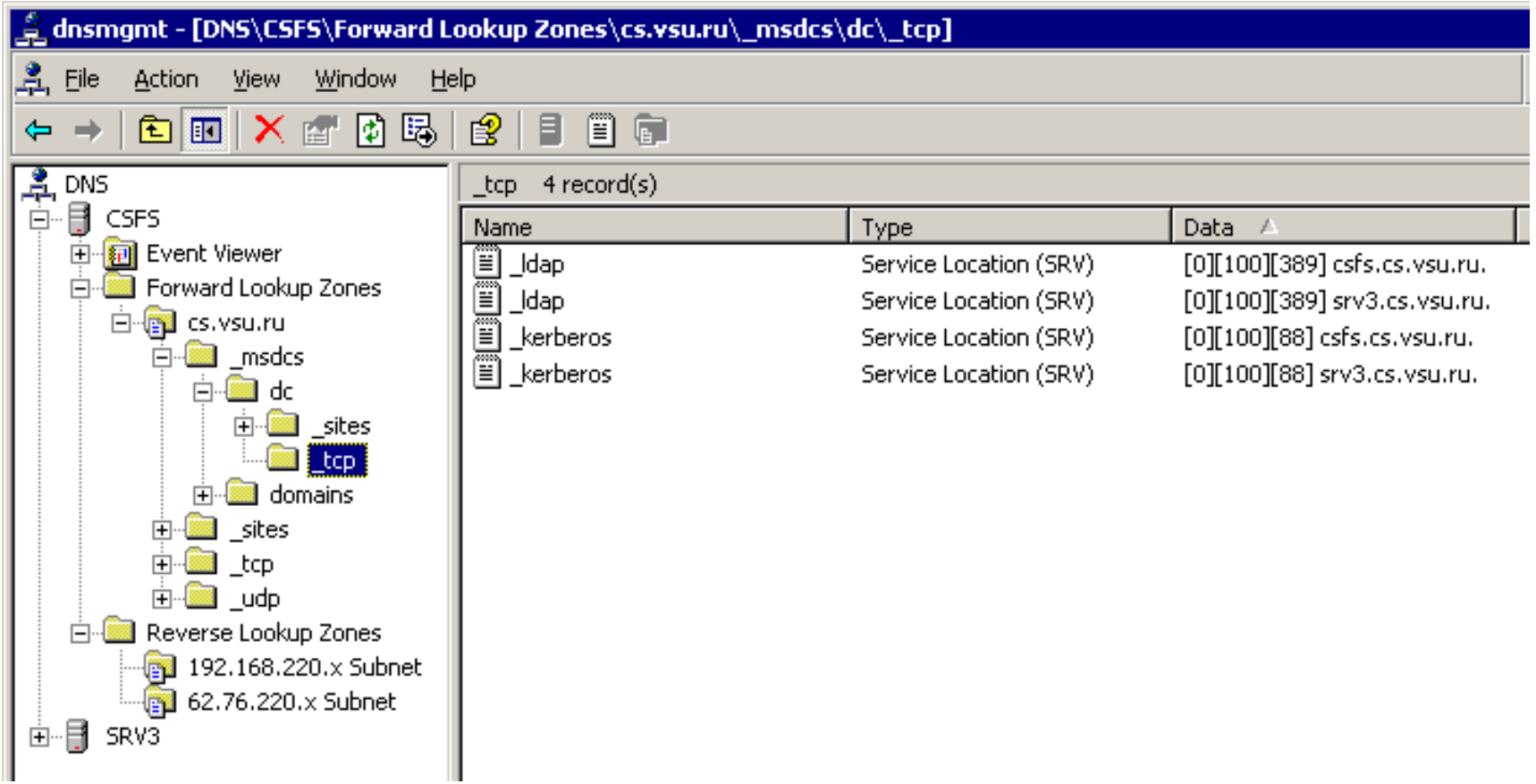
Динамическая служба DNS

- Динамический DNS (DDNS) – возможность авто-обновлений содержимого DNS, RFC2136
- Логика обновлений
  - Загрузка компьютера
  - Получение адреса от DHCP
  - передача данных о компьютере в DDNS
- Адреса DNS
  - FQDN, Fully Qualified Domain Name
    - Пример www.cs.vsu.ru
    - www – имя узла, cs - имя домена 3 уровня, vsu - имя домена 2 уровня, ru - имя домена верхнего уровня
  - RDN, Relative Distinguished/Domain Name или Hostname
    - www – относительное имя (узла, hostname) в домене cs.vsu.ru

Обычные адресные записи DNS в прямой зоне



Новые типы записей (SRV) DNS для поддержки AD



Домены

- Домен AD использует общую политику защиты и те же самые локальные и глобальные группы домена.
- Домен служит границей репликации: AD допускает репликацию объектов домена только на контроллеры данного домена

Физическая структура AD: контроллеры домена, сайты

- Контроллер домена (DC) – хранитель копии БД Active Directory
  - управляет доступом и изменяет данные AD
  - аутентифицирует пользователей, раздает пользователям маркеры безопасности (security token), содержащие список групп, права
- Хозяин операций (operation master) – сервер(ы), следящий за тем, чтобы изменения схемы AD не конфликтовали. Хозяин операций функционирует на уровне домена и на уровне леса доменов. Существует 5 (Flexible Single Master Operations, FSMO) ролей, назначаемых на конкретные DC.
- Сайт – несколько IP подсетей, соединенных высокоскоростными каналами. Эта информация учитывается при репликации AD, при нахождении локального контроллера домена.

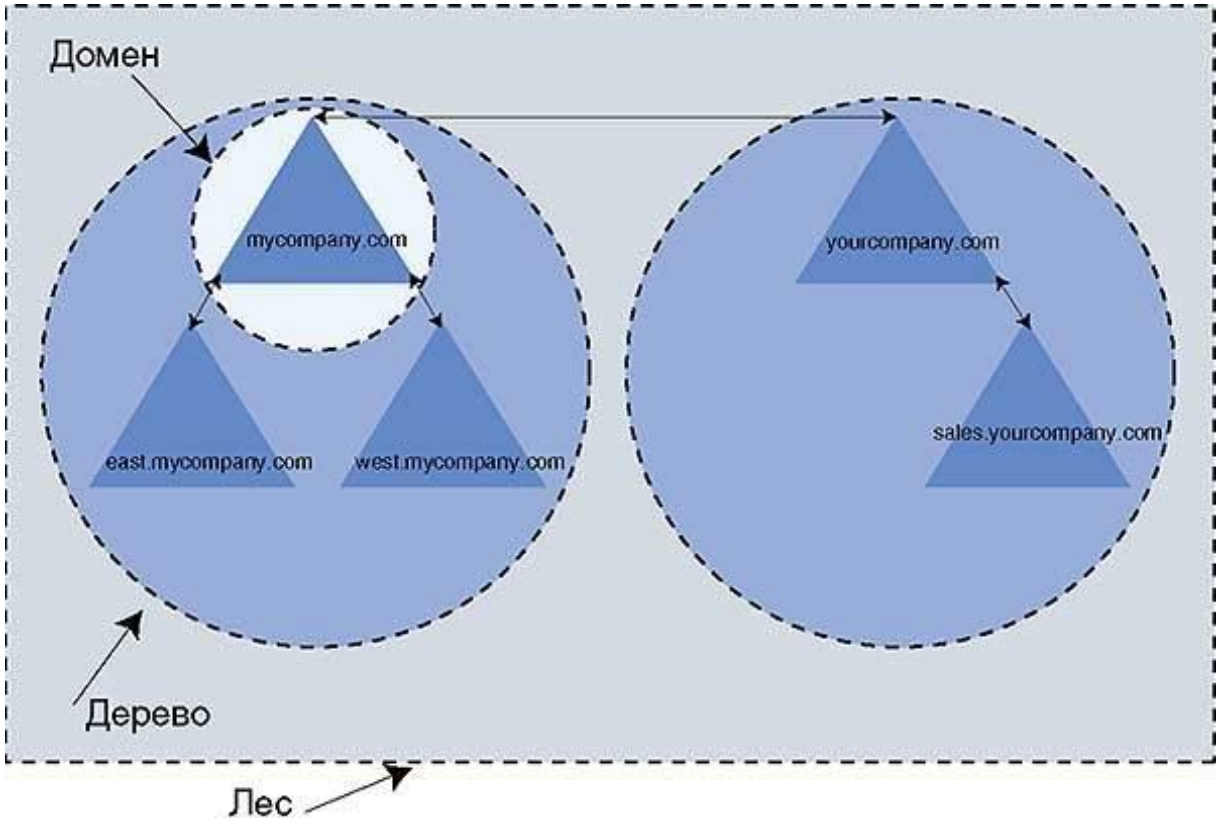
Дерево доменов

- Дерево доменов – иерархия доменов, которые являются частью общего пространства имен DNS
- vsu.ru
  - main.vsu.ru
    - www.main.vsu.ru
  - is.vsu.ru
  - cs.vsu.ru
    - csfs.cs.vsu.ru
    - srv3.cs.vsu.ru

Лес доменов

- Лес представляет собой одно или несколько деревьев доменов, использующих общую схему и общую границу защиты
- В пределах леса действуют транзитивные доверительные отношения объединяющие все домены
- По отношению к «чужим» доменам лес может устанавливать доверительные нетранзитивные отношения

Домены, деревья и леса AD



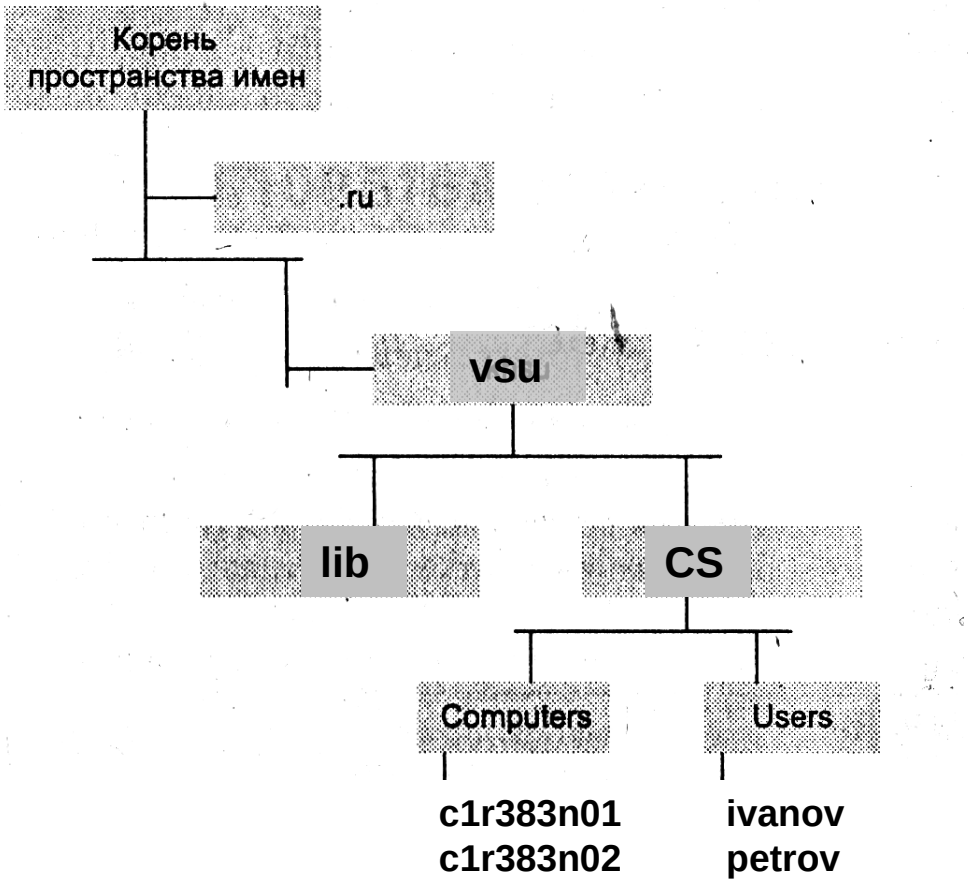
Определяя количество доменов и планируя структуру деревьев доменов и лесов, следует рассматривать политические, организационные, географические и технические факторы

Затраты дискового пространства для объектов AD

Объект	Необходимое дисковое пространство
Дополнительный атрибут объекта (для 10-символьной строки)	100 байт
OU	1,1 Кбайт
Пользователь (только набор обязательных атрибутов)	3,7 Кбайт

Предлагаемый компанией Microsoft продукт Active Directory Sizer поможет определить технические характеристики контроллера домена для разработанного проекта конфигурации каталога AD. Продукт можно получить по адресу: *http://www.microsoft.com/windows2000/library/planning/activedirectory/adsizer.asp*.

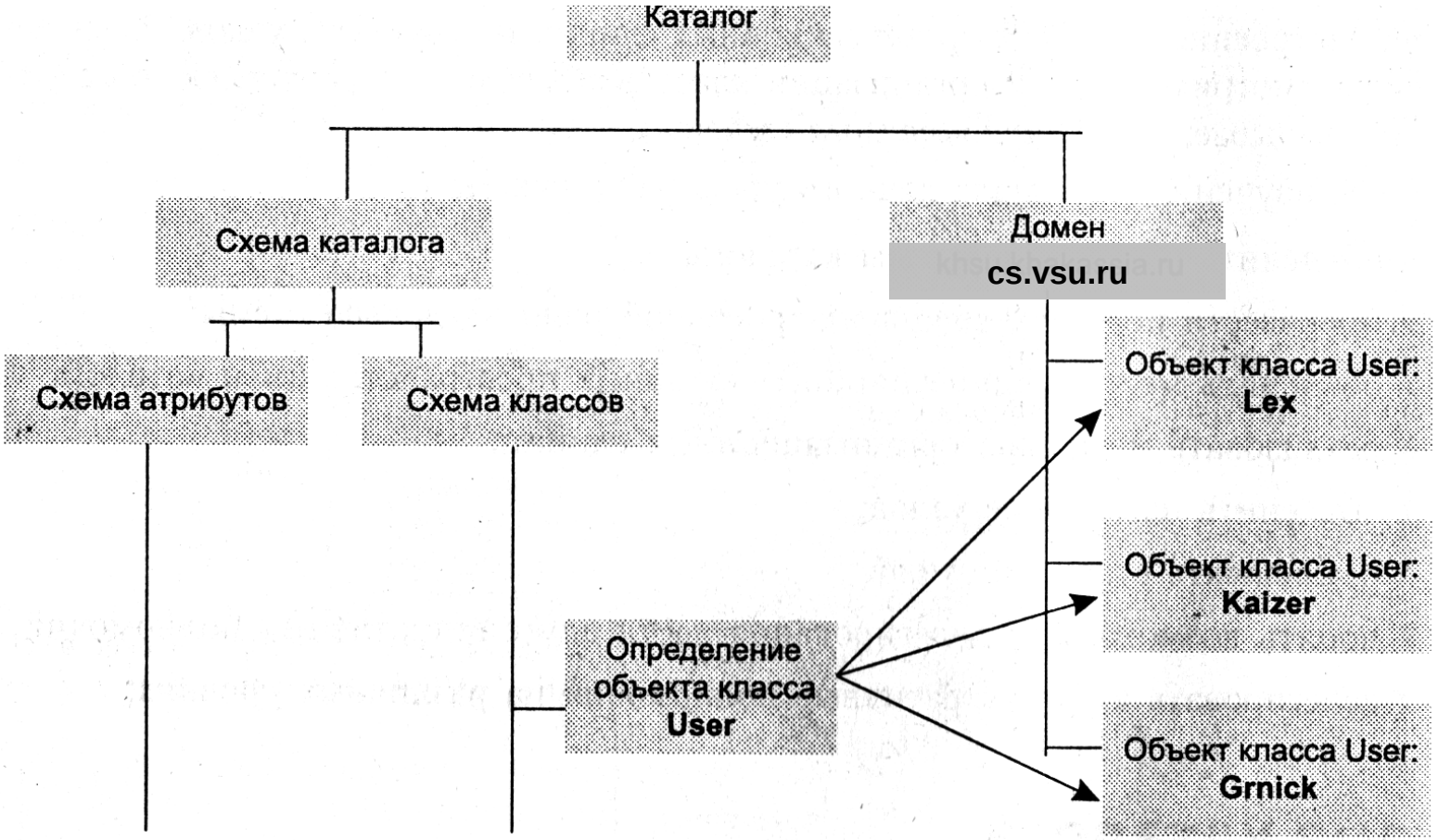
Пространство имен AD

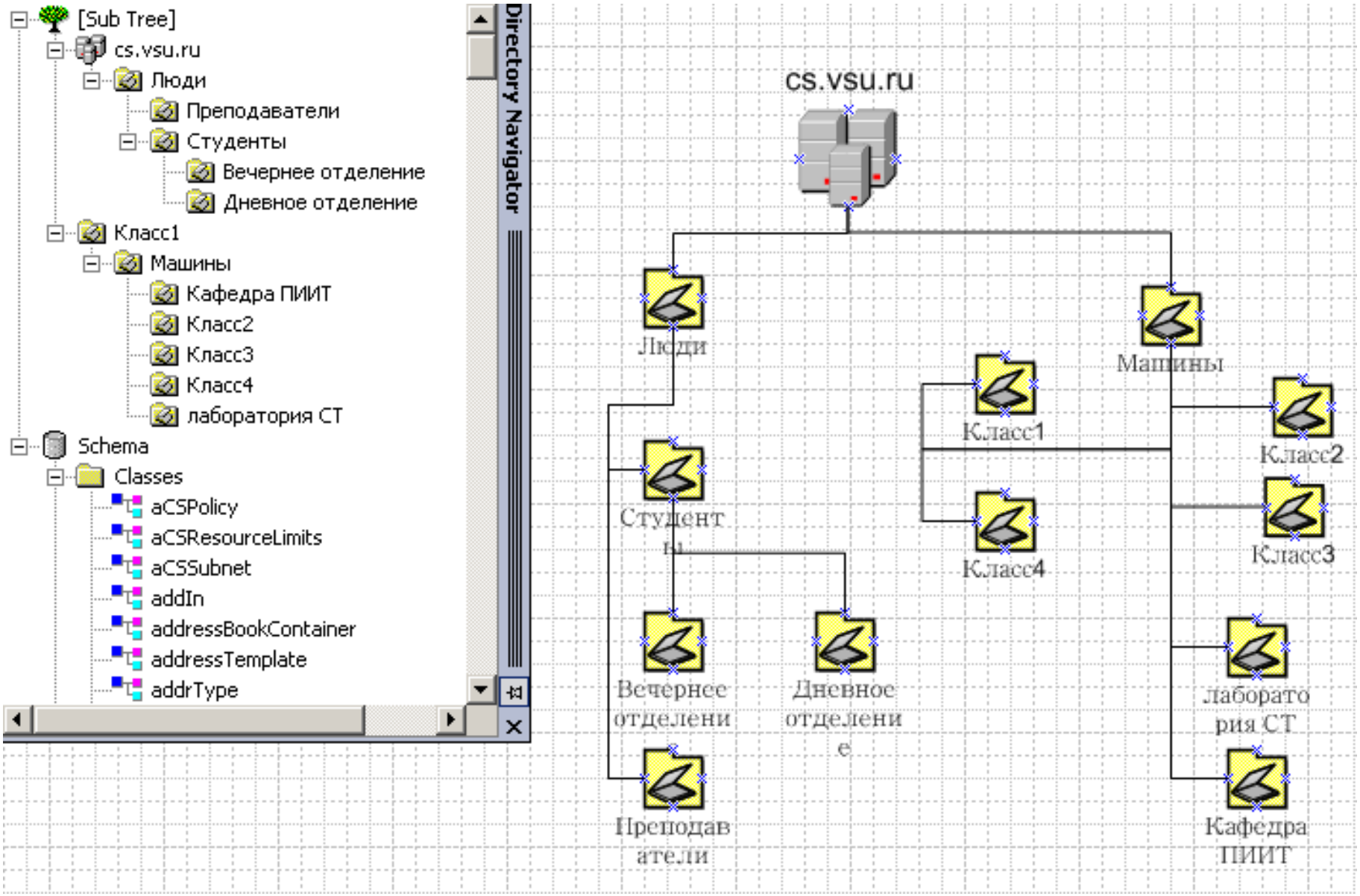


Состав AD

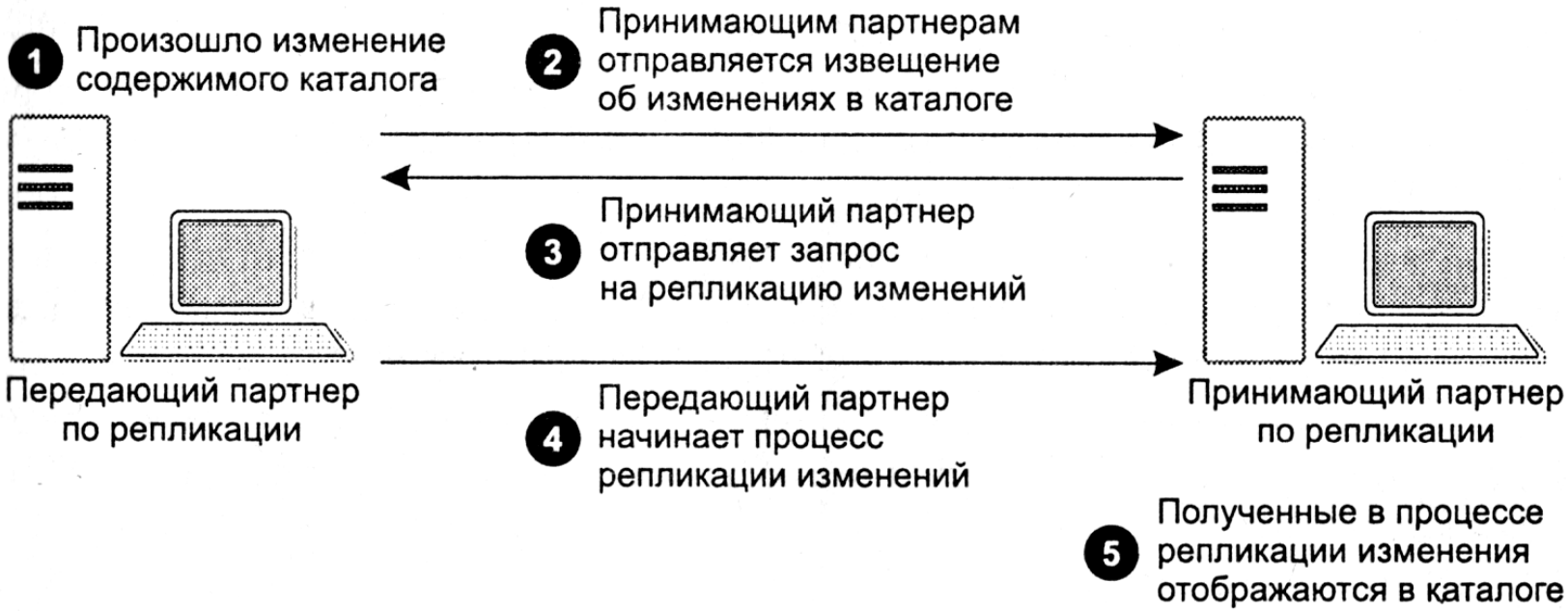
- Объекты
  - groups
  - computers
  - domains
  - cites
  - …
- Схема AD - иерархическая структура объектов

Схема AD


Каталог
Схема каталога
Домен
cs.vsu.ru
Схема атрибутов
Схема классов
Объект класса User:
Lex
Объект класса User:
Kaizer
Определение
объекта класса
User
Объект класса User:
Grnick

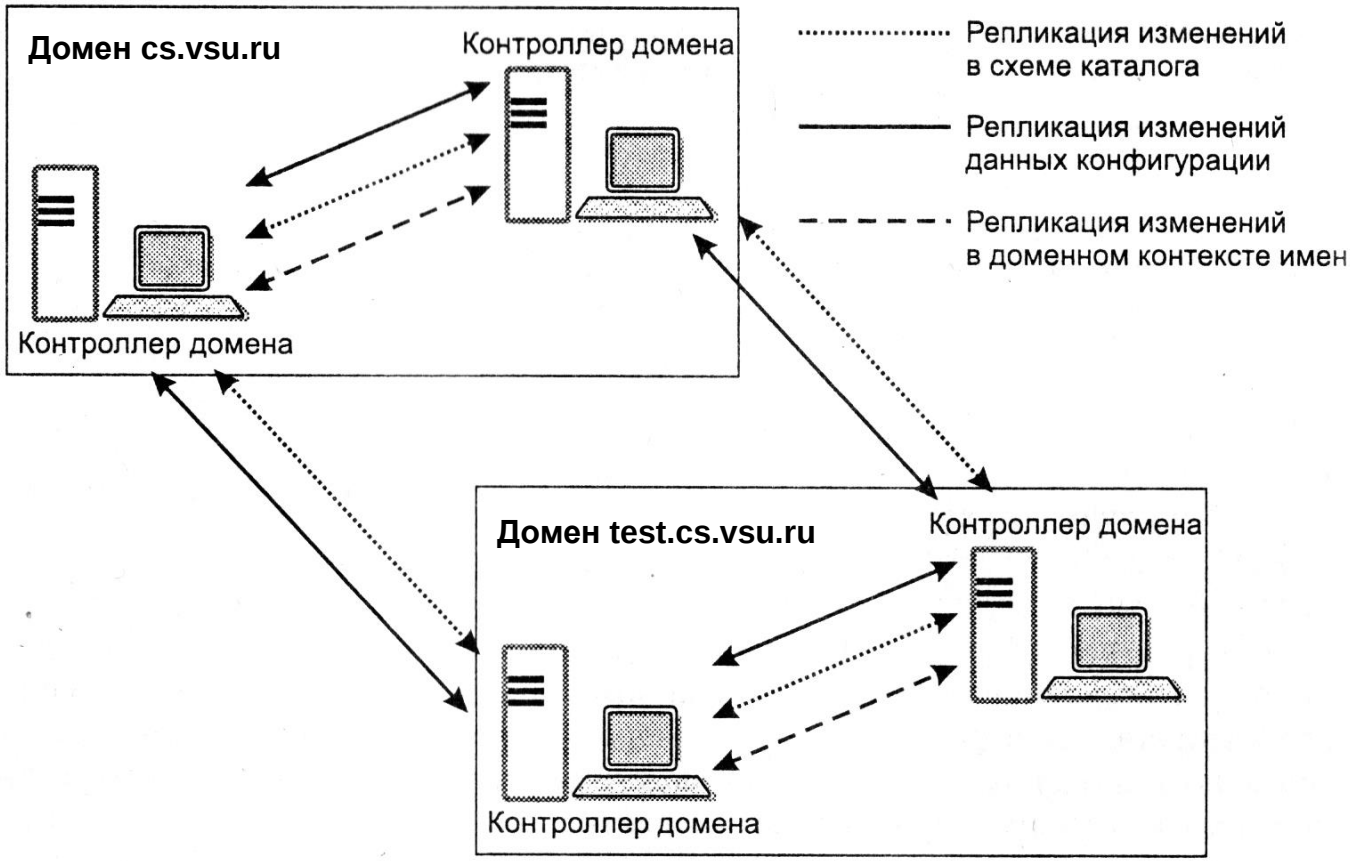

[Sub Tree]
cs.vsu.ru
Люди
Преподаватели
Студенты
Вечернее отделение
Дневное отделение
Класс1
Машины
Кафедра ПИИТ
Класс2
Класс3
Класс4
лаборатория СТ
Schema
Classes
aCSPolicy
aCSResourceLimits
aCSSubnet
addIn
addressBookContainer
addressTemplate
addrType
Directory Navigator
cs.vsu.ru
Люди
Машины
Класс1
Класс2
Студенты
Класс4
Класс3
Вечернее отделение
Дневное отделение
лаборатория СТ
Преподаватели
Кафедра ПИИТ

Процесс репликации

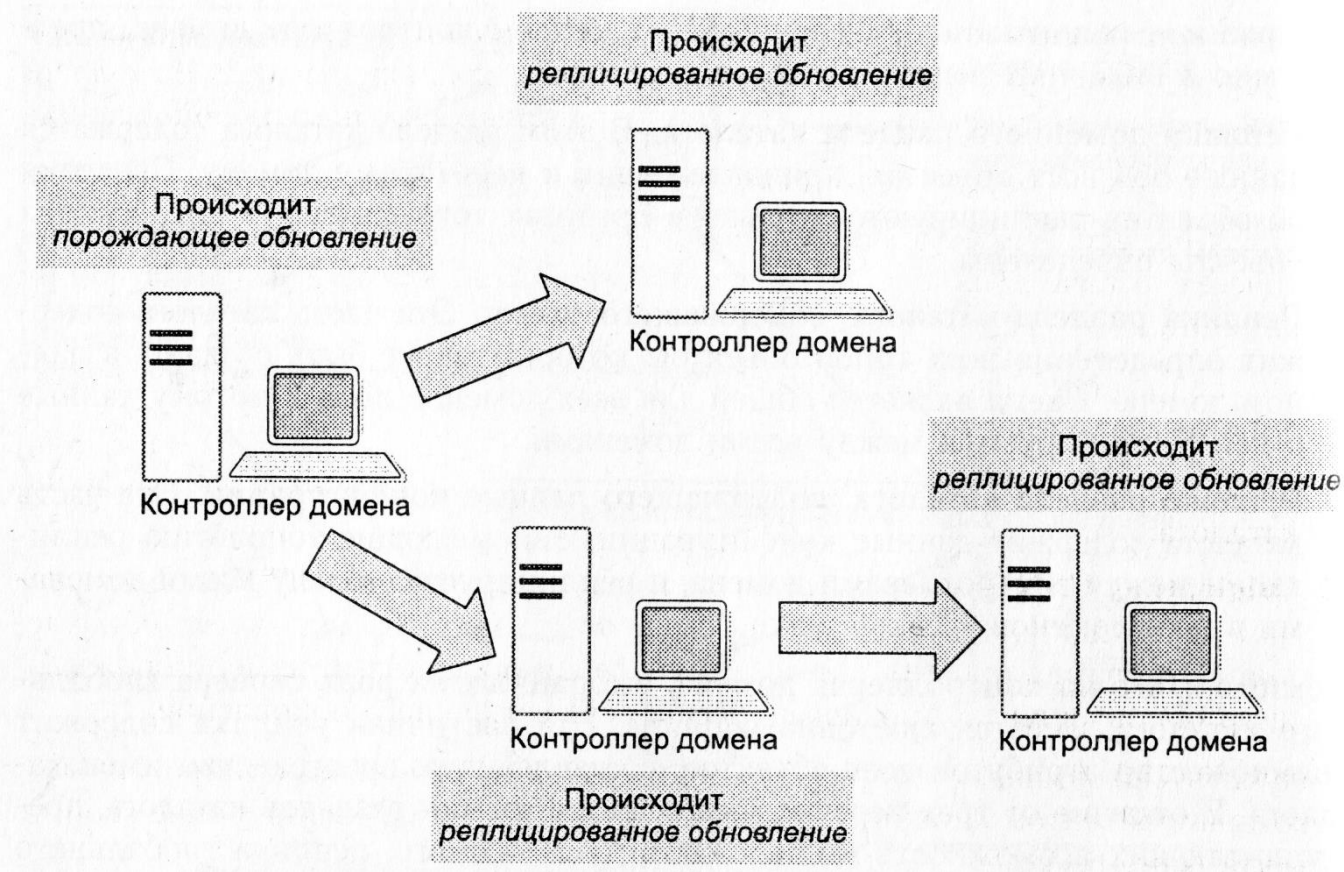


Модель репликации - multi-master

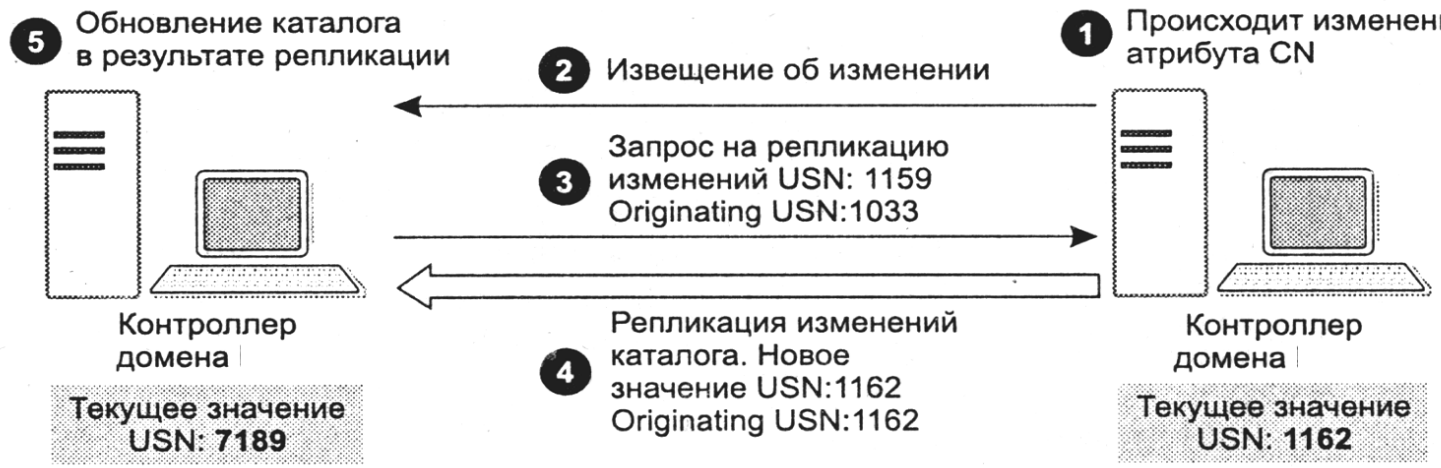
Репликация в различных контекстах имени каталога



Распространение обновления



Отслеживание последних изменений (USN, update sequence numbers)



При помощи двух дополнительных компонентов: вектора **High-watermark** и вектора **Up-to-dateness** определяется какие именно объекты и атрибуты существующих нужно забирать.

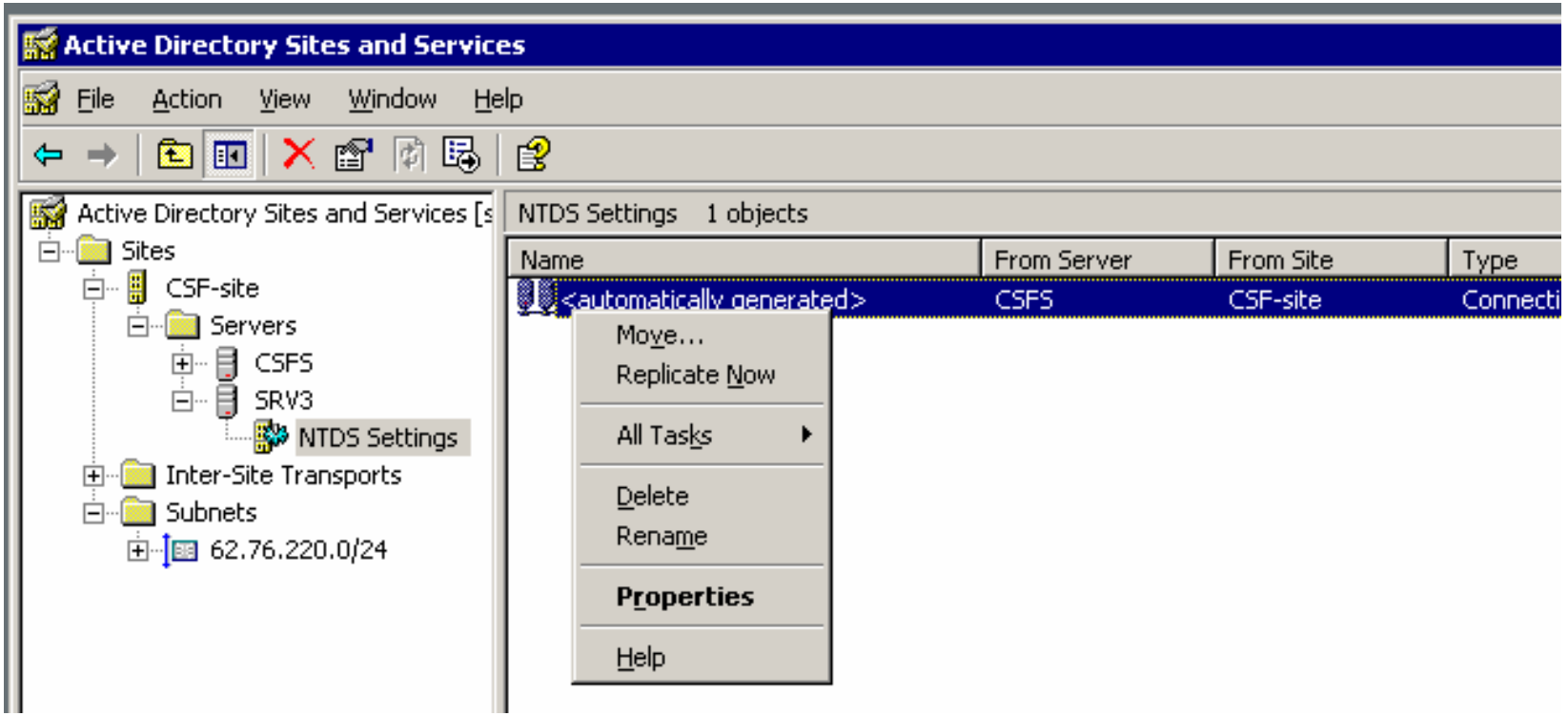
High-watermark вектор содержит максимальные USN партнеров

Up-to-dateness вектор содержит максимальные значения оригинальных USN (номера последней первичной операции записи) всех контроллеров с их GUID

Репликационная информация объекта в AD

uSNCreated USN операции записи создания объекта в данной реплике					
uSNChanged USN операции записи изменения объекта в данной реплике					
Атрибут	Локальный USN	Версия атрибута	Время обновления	Оригинальный USN	GUID контроллера обновления
Атрибут	Локальный USN	Версия атрибута	Время обновления	Оригинальный USN	GUID контроллера обновления
Атрибут	Локальный USN	Версия атрибута	Время обновления	Оригинальный USN	GUID контроллера обновления
Атрибут	Локальный USN	Версия атрибута	Время обновления	Оригинальный USN	GUID контроллера обновления

Консоль управления «сайты и службы»



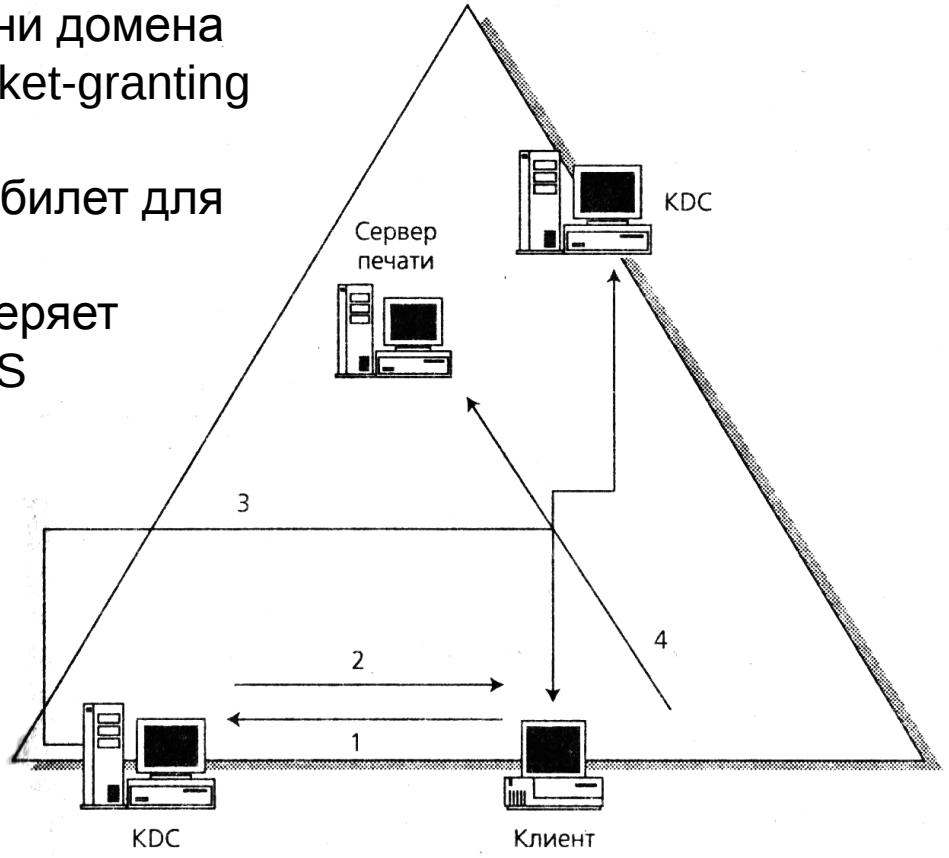
Kerberos – открытый стандарт, разработанный в MIT

Субъекты протокола:

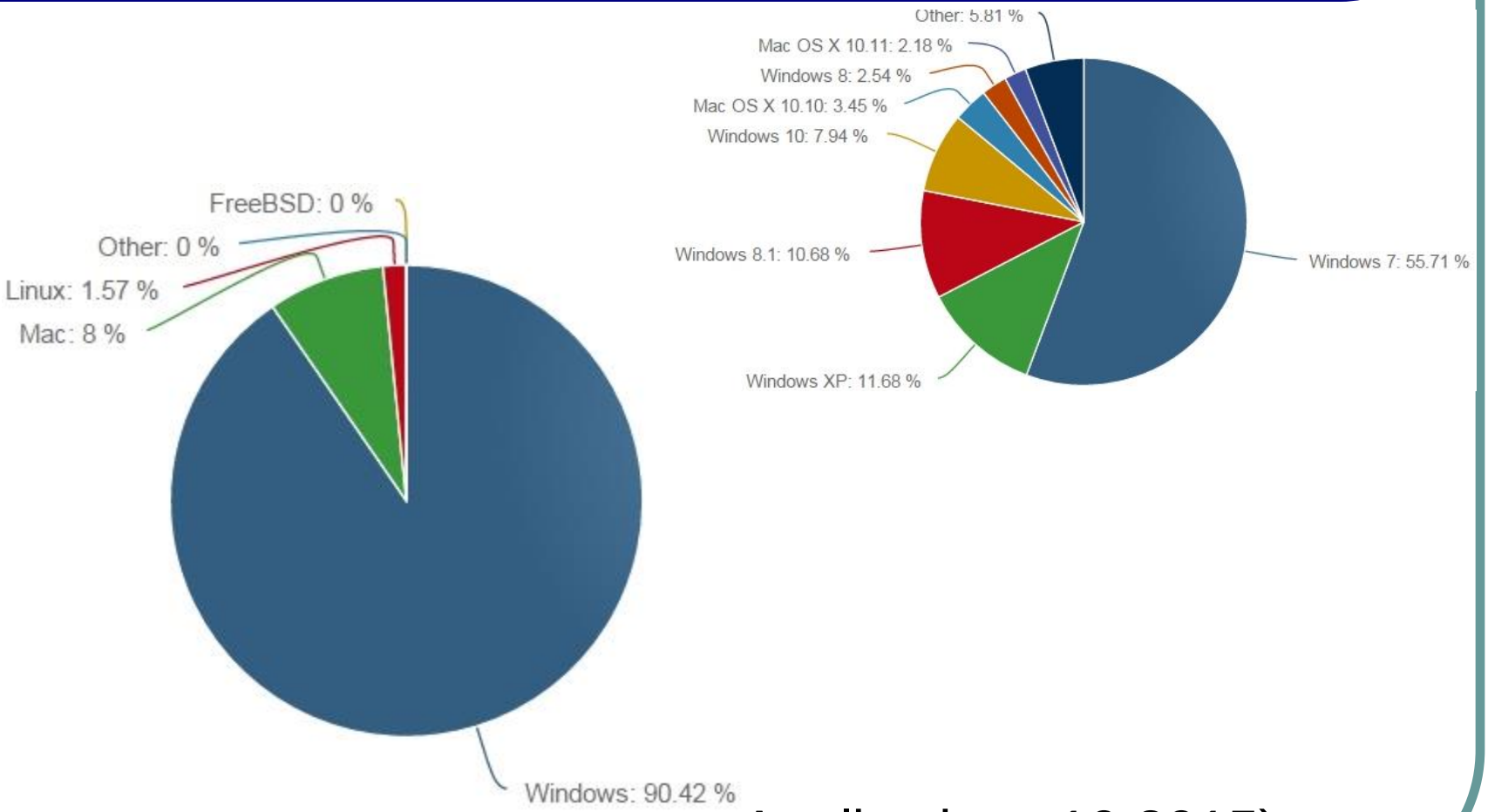
- Пользователь (User)
- Сервер (Server)
- Центр распространения ключей (KDC)

Этапы, транзакции Kerberos

1. ввод имени, пароля, имени домена выдается билет TGT – ticket-granting ticket
2. по TGT билету выдается билет для службы –TGS
3. сервер приложения проверяет возможности данного TGS



Клиентские ОС Microsoft



статистика (данные Net Applications 10.2015)

Клиентские ОС Microsoft

Статистика клиентских ОС сообщества STEAM, 10.2015:

1. Windows 7: 44,42 %;
2. Windows 10: 27,64 %;
3. Windows 8.1: 18,06 %;
4. Mac OS X: 3,54 %;
5. Windows 8: 2,46 %;
6. Windows XP: 2,24 %;
7. Linux: 0,98 %;
8. Windows Vista: 0,52 %.

Ссылки

- 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”