



Введение

Лекция 1

План лекции

- Понятие, цель и задачи сетевого администрирования
- Семейство операционных систем Windows Server 2008
- Сравнение редакций Windows Server
- Инструменты администрирования

Понятие, цель и задачи сетевого администрирования

Цель создания любой компьютерной сети – предоставление доступа к её ресурсам.

Виды ресурсов:

- ☐ данные (файлы и папки)
- ☐ устройства (принтеры, сканеры, модемы)
- ☐ вычислительные возможности, обеспечиваемые процессорами

Понятие, цель и задачи сетевого администрирования

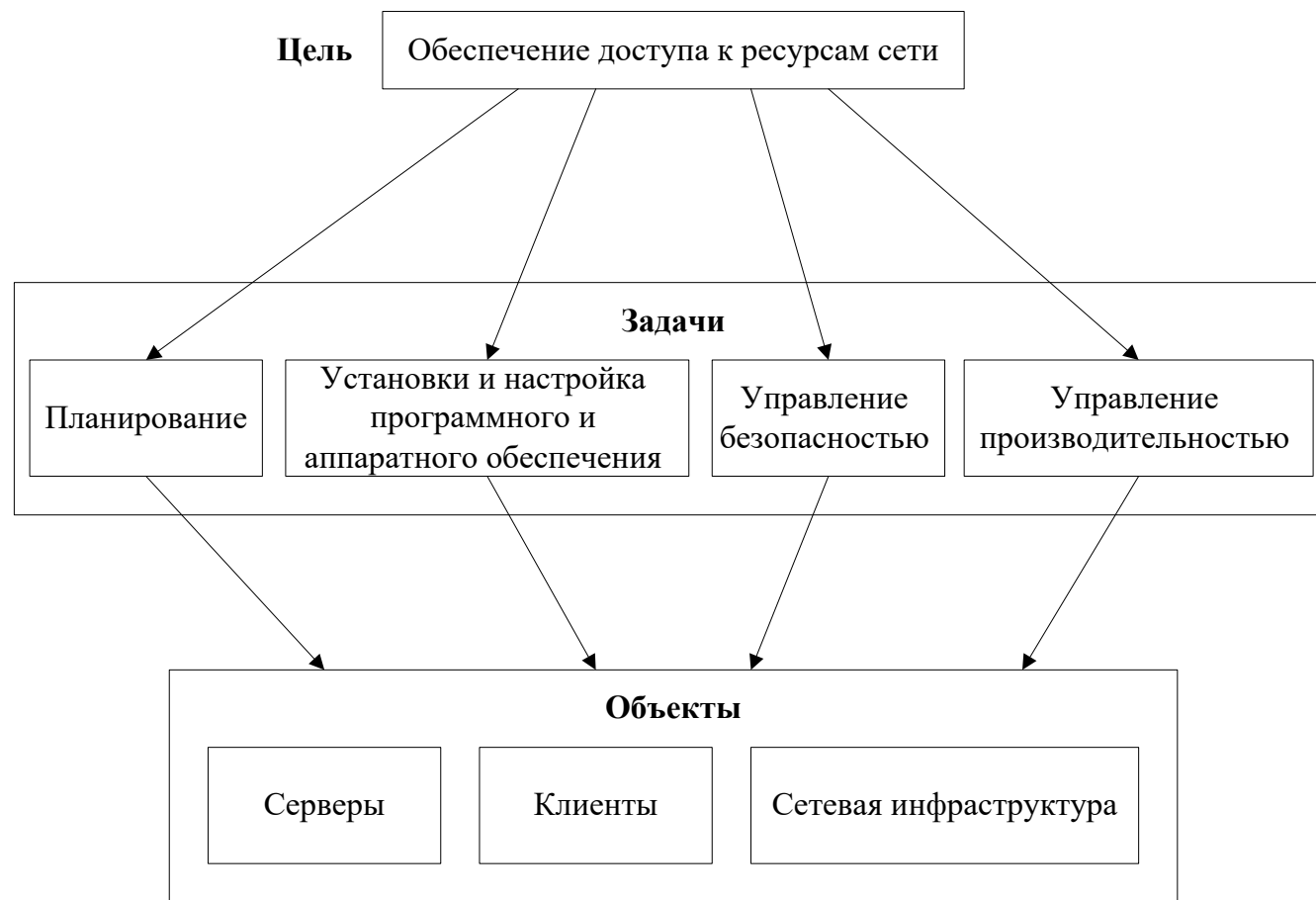
- *Сетевое администрирование* – управление ресурсами и инфраструктурой сети для обеспечения эффективного, надежного и безопасного доступа к её ресурсам.

Понятие, цель и задачи сетевого администрирования

Группы задач сетевого администрирования:

- задачи планирования
- задачи установки и настройки программного и аппаратного обеспечения
- задачи управления безопасностью
- задачи управления производительностью

Понятие, цель и задачи сетевого администрирования



Семейство операционных систем Windows Server 2008

Версии Microsoft Windows Server 2008:

- Windows Server 2008 Standard Edition (стандартная версия)
- Windows Server 2008 Enterprise Edition (корпоративная версия)
- Windows Server 2008 Datacenter Edition (версия для центра обработки данных)
- Windows Server 2008 Web Edition (версия для web-узлов)

Семейство операционных систем Windows Server 2008

Сравнение различных выпусков Windows Server 2008

Возможность	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Число поддерживаемых процессоров	До 4	До 8	До 32 на платформе x86 До 64 на платформе x64	До 4
Количество поддерживаемой памяти	До 4 Гбайт на платформе x86 До 32 Гбайт на платформе x64	До 64 Гбайт на платформе x86 До 2 Тбайт на платформе x64	До 64 Гбайт на платформе x86 До 2 Тбайт на платформе x64	До 4 Гбайт на платформе x86 До 32 Гбайт на платформе x64
Кластеризация	Нет	До 16 узлов	До 16 узлов	Нет
Права на использование виртуальных машин	1 VM	До 4 VM	Не ограничены	Не поддерживается

Принципы лицензирования

Windows Server 2008 лицензируется по схеме лицензия на Сервер (или на процессор) + лицензия клиентского доступа CAL + дополнительная лицензия External Connector.

- ❖ Для редакций Standard и Enterprise требуется лицензия "на сервер"
- ❖ Для редакций Datacenter и Itanium требуется лицензия "на процессор"

Редакция Windows Web Server 2008 не требует лицензий клиентского доступа.

^[1] Каждому пользователю или устройству, которые обращаются к серверу, требуются лицензии клиентского доступа (Client Access Licenses, CAL). См. Product Use Rights («Права на использование продукта») для получения более подробной информации.

Сравнение редакций Windows Server 2012

	Datacenter	Standard	Essentials	Foundation
Применение	Для сред с высокой степенью виртуализации	Для сред с низкой степенью или отсутствием виртуализации.	Для организаций малого бизнеса	
Доступные возможности и технологии	Все функциональные возможности		Ограниченный набор возможностей	
Права на использование виртуализации	Неограниченное число виртуальных машин	Не более двух виртуальных машин	Может быть гостевой VM	Только в среде физической ОС
Модель лицензирования	На процессор (одна лицензия покрывает 2 процессора) + CAL		На сервер (только 1- и 2-процессорные серверы). Не более 25 пользователей.	На сервер (только однопроцессорные серверы). Не более 15 пользователей.

Сравнение возможностей Windows Server 2012 и 2012 R2 с версией Windows Server 2016

Описание	Windows Server 2012 и 2012 R2 (Standard и Datacenter)	Windows Server 2016 (Standard и Datacenter)
Объем памяти на физических серверах	До 4 ТБ на один физический сервер	До 24 ТБ на один физический сервер (в 6 раз больше)
Количество логических процессоров на физических серверах	До 320 логических процессоров	До 512 логических процессоров
Объем памяти в виртуальной машине	До 1 ТБ	До 16 ТБ (в 16 раз больше)
Количество виртуальных процессоров в виртуальной машине	До 64	До 240 (в 3,75 раза больше)

Инструменты администрирования

Инструменты:

- Графические инструменты
 - *Диспетчер серверов*
 - *Консоль управления Microsoft (Microsoft Management Console, MMC)*
 - *Административные мастера*
- *Утилиты командной строки*
- *Windows PowerShell*



Протокол DNSP

Лекция 2

План лекции

- Проблема автоматизации распределения IP-адресов
- Реализация DHCP в Windows
- Параметры DHCP
- Адреса для динамической конфигурации
- DHCP-сообщения
- Принцип работы DHCP
- Авторизация DHCP-сервера

Проблема автоматизации распределения IP-адресов

- DHCP
 - Dynamic Host Configuration Protocol
(протокол динамической конфигурации хоста)
- RFC 2131

Реализация DHCP в Windows

- *Область действия (scope)*
- *Аренда (lease)*

Параметры DHCP

Основные параметры (RFC 2132):

- Subnet mask
- Router
- Domain Name Servers
- DNS Domain Name
- WINS Server Names
- Lease Time
- Renewal Time (T1)
- Rebinding Time (T2)

Параметры DHCP

Уровни применения параметров:

- уровень сервера
- уровень области действия
- уровень класса
(**IPconfig /setclassid**)
- уровень клиента
(для зарезервированных адресов)

Адреса для динамической конфигурации

Диапазоны *частных адресов*

(Private addresses, RFC 1918):

- ID подсети – 10.0.0.0
маска подсети: 255.0.0.0
- ID подсети – 172.16.0.0
маска подсети: 255.240.0.0
- ID подсети – 192.168.0.0
маска подсети: 255.255.0.0

Адреса для динамической конфигурации

Диапазон *автоматических частных адресов*

APIPA (Automatic Private IP Address):

- ☐ ID подсети – 169.254.0.0
- ☐ маска подсети: 255.255.0.0

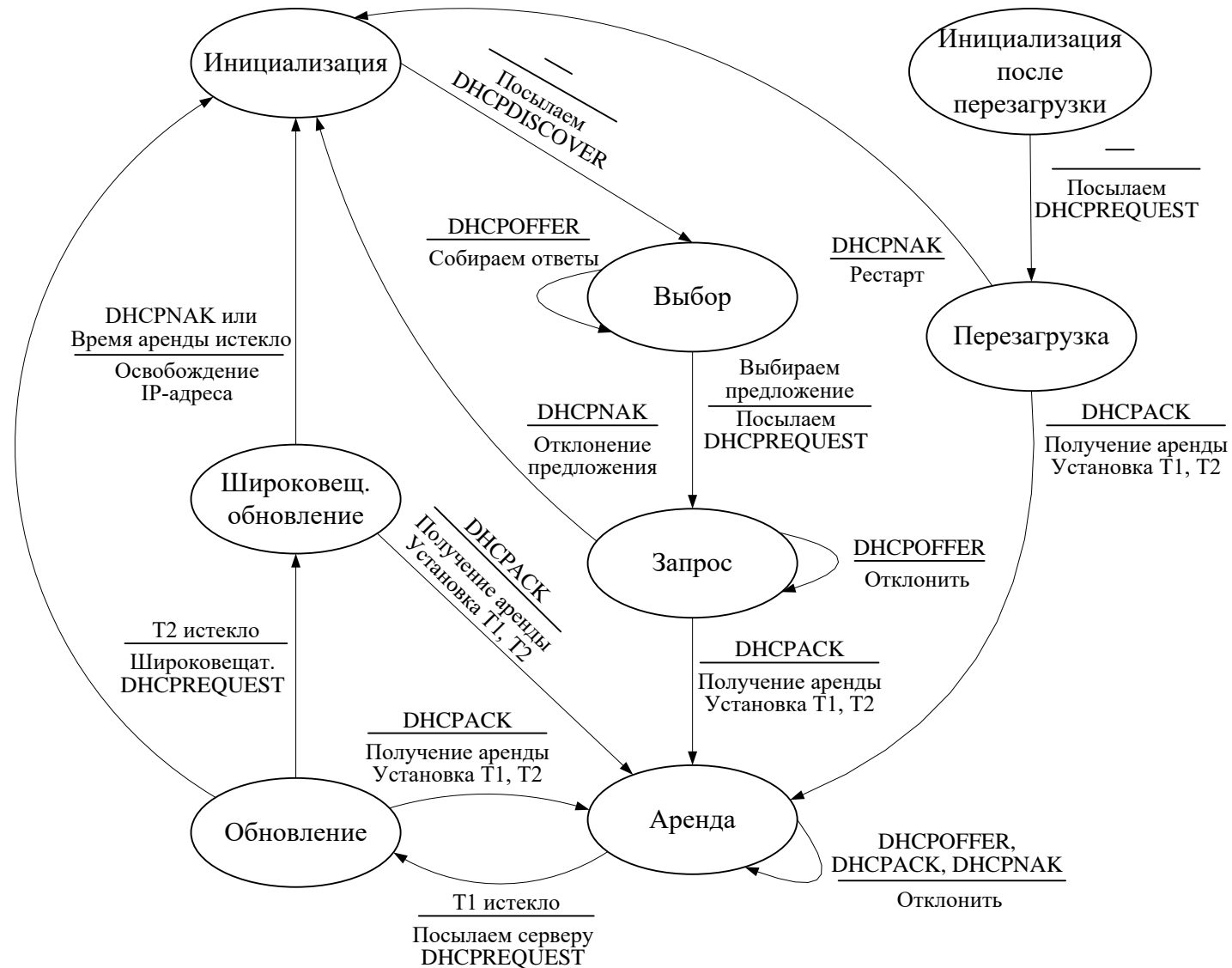
DHCP-сообщения

Тип сообщения	Направление	Значение
DHCPDISCOVER (DHCP-обнаружение)	Клиент → сервер	Широковещательный запрос для обнаружения DHCP-сервера
DHCPOFFER (DHCP-предложение)	Сервер → клиент	Ответ на DHCPDISCOVER, содержит предлагаемые сетевые параметры
DHCPREQUEST (DHCP-запрос)	Клиент → сервер	Запрос предложенных параметров
DHCPACK (DHCP-подтверждение)	Сервер → клиент	Подтверждение сетевых параметров

DHCP-сообщения

Тип сообщения	Направление	Значение
DHCPNAK (DHCP-несогласие)	Сервер → клиент	Отклонение запроса клиента
DHCPDECLINE (DHCP-отказ)	Клиент → сервер	Отказ клиента от предложенных параметров
DHCPRELEASE (DHCP-освобождение)	Клиент → сервер	Освобождение арендованного IP-адреса
DHCPINFORM (DHCP-информация)	Клиент → сервер	Запрос дополнительных параметров

Принцип работы DHCP



Авторизация DHCP-сервера

Для предотвращения несанкционированного использования DHCP-серверов в сетях Active Directory применяется *механизм авторизации*.

Системный администратор регистрирует IP-адрес сервера в каталоге Active Directory.



Имена в ТСР/IP

Лекция 3

План лекции

- Необходимость символьных имен
- Система доменных имен
- Процесс разрешения имен
- Записи о ресурсах
- Утилита NSLOOKUP
- Имена NetBIOS и служба WINS
- Протокол LLMNR
- Punycode
- DNSSEC

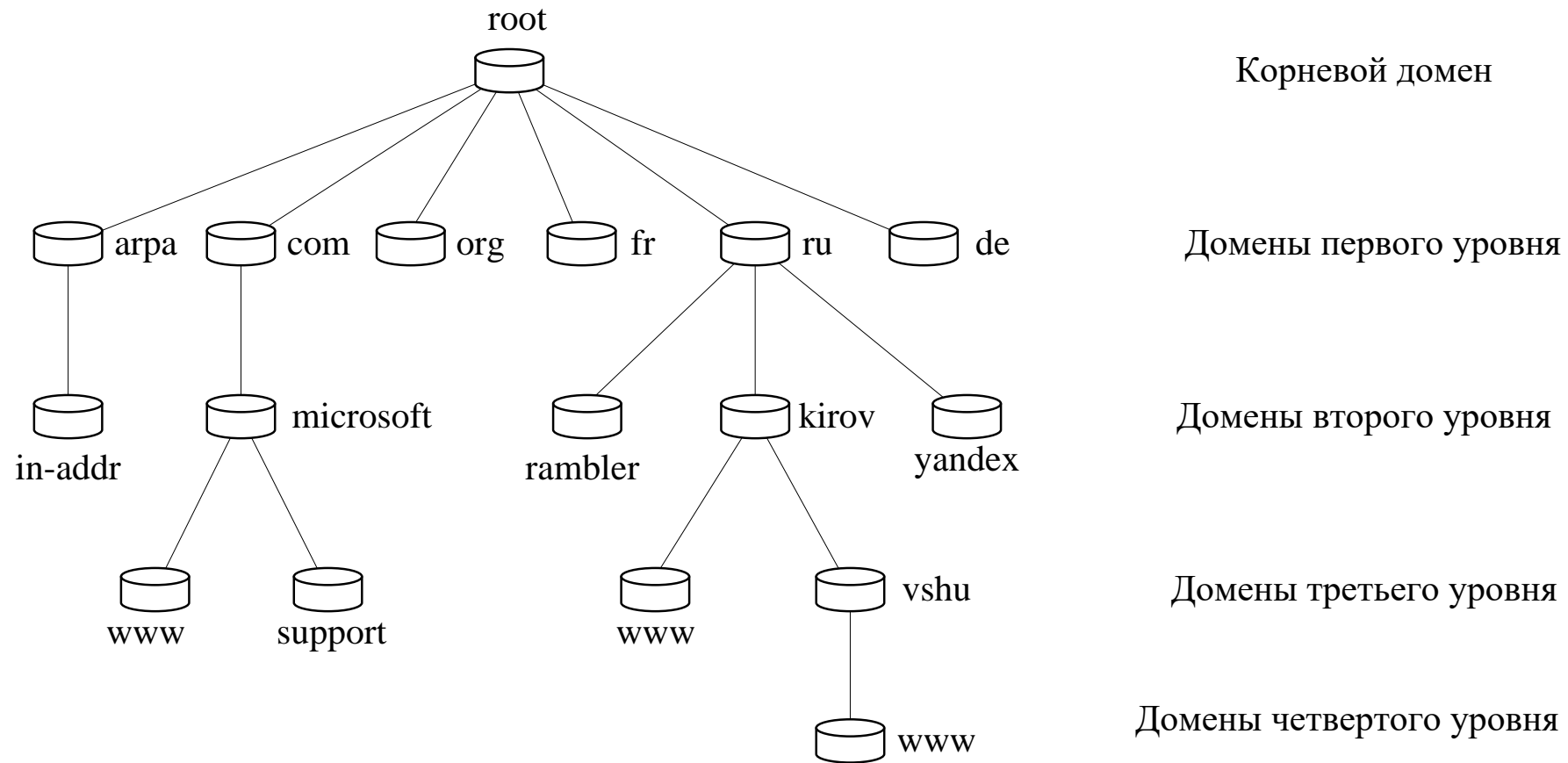
Необходимость символьных имен

Система доменных имен DNS
(Domain Name System)

описывается в RFC 1034 и RFC 1035.

Полное название доменных имен – FQDN (Fully Qualified Domain Name – полностью определенное имя домена).

Система доменных имен



Система доменных имен

Полностью определенное доменное имя FQDN записывается следующим образом:

- ☐ имя хоста
- ☐ DNS-суффикс
- ☐ точка (корневой домен)

Пример FQDN для хоста **www** домена **vshu**:
www.vshu.kirov.ru.

- ☐ **www** – имя хоста
- ☐ **vshu.kirov.ru.** – DNS-суффикс
- ☐ Точку в конце FQDN обычно можно опускать

Файл Hosts

```
# (C) Корпорация Майкрософт (Microsoft Corp.), 1993-1999
#
# Это образец файла HOSTS, используемый Microsoft TCP/IP для Windows.
#
# Этот файл содержит сопоставления IP-адресов именам узлов.
# Каждый элемент должен располагаться в отдельной строке. IP-адрес должен
# находиться в первом столбце, за ним должно следовать соответствующее имя.
# IP-адрес и имя узла должны разделяться хотя бы одним пробелом.
#
# Кроме того, в некоторых строках могут быть вставлены комментарии
# (такие, как эта строка), они должны следовать за именем узла и отделяться
# от него символом '#'.
#
# Например:
#
#      102.54.94.97      rhino.acme.com      # исходный сервер
#      38.25.63.10      x.acme.com         # узел клиента x
#
127.0.0.1 localhost
127.0.0.1 activate.adobe.com
```

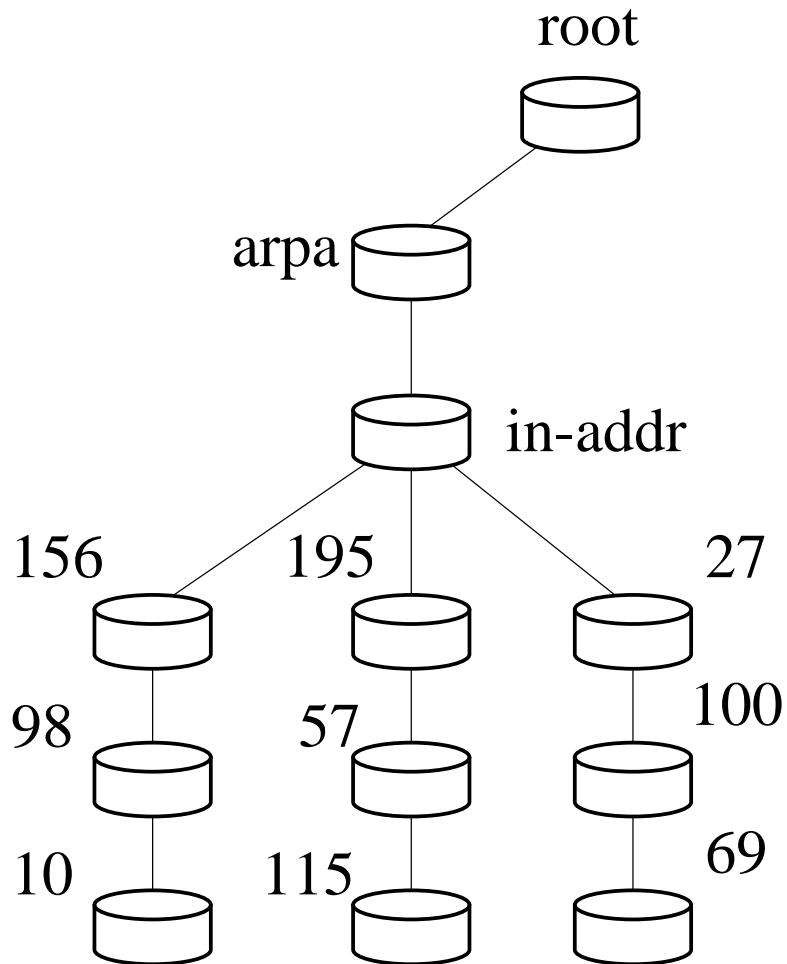
- *%systemroot%\system32\drivers\etc*
- *c:\Windows\system32\drivers\etc*

Служба DNS

Служба в TCP/IP, которая занимается переводом доменного имени в IP-адрес и обратно, называется *Domain Name Service* – служба доменных имен.

Процесс преобразования доменного имени в IP-адрес называется *разрешением доменного имени*.

Служба DNS



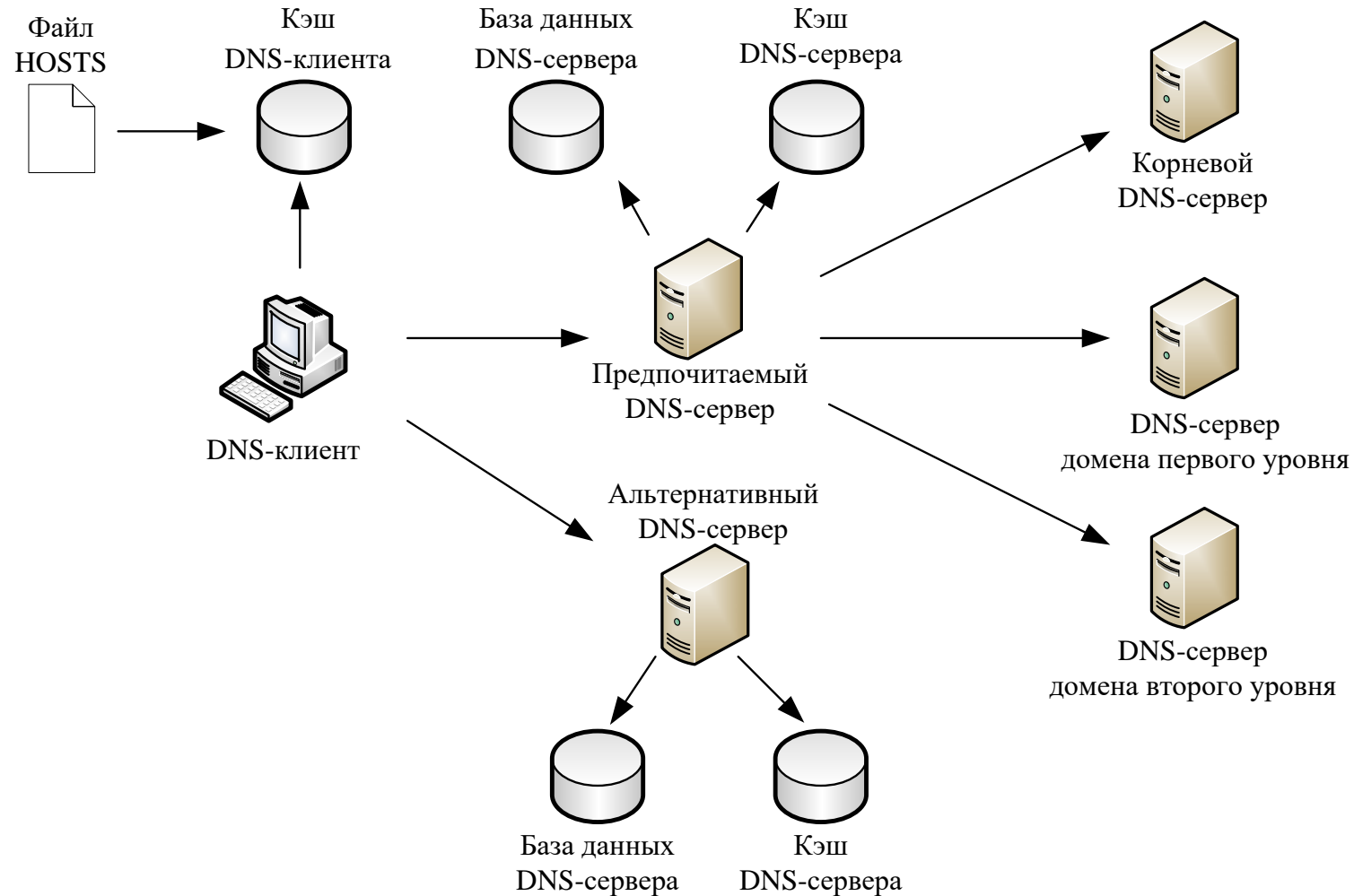
Зона обратного преобразования, соответствующая подсети 156.98.10.0 будет называться **10.98.156.in-addr.arpa.**

Процесс разрешения имен

Системный компонент DNS-клиента, называемый *DNS-распознавателем*, отправляет запросы на DNS-серверы. Запросы бывают двух видов:

- *итеративные*
- *рекурсивные*

Процесс разрешения имен



Записи о ресурсах

Наиболее важные типы записей о ресурсах (resource record):

- A (Host Address – адрес хоста)
- CNAME (Canonical Name – псевдоним)
- MX (Mail Exchanger – почтовый обменник)
- NS (Name Server – сервер имен)
- PTR (Pointer – указатель)
- SOA (Start Of Authority – начало авторизации)
- SRV (Service Locator – определитель служб)

Записи о ресурсах

- A – сопоставляет доменному имени IP-адрес (IPv4)
- AAAA или A6 – сопоставляет доменному имени IP-адрес (IPv6)
- PTR – сопоставляет IP-адресу доменное имя узла
- CNAME – определение псевдонима DNS-имени

mail.unn.ru.	IN	CNAME	ns.unn.ru.
ns.unn.ru.	IN	A	1.2.3.4
ns2	IN	A6	1.2.3.4.5.6.7.8
4.3.2.1.in-addr.arpa.	IN	PTR	ns.unn.ru.

Записи о ресурсах

- MX – определяет имя почтового сервера для указанного доменного имени (почта, отправленная на адрес user@unn.ru будет отправляться именно на этот сервер)
 - можно указать несколько почтовых серверов и их относительные приоритеты после поля "тип записи" (чем меньше численное значение, тем выше приоритет)

unn.ru.	IN	MX	0	mail.unn.ru.
*.unn.ru.	IN	MX	0	mail.unn.ru.
unn.ru.	IN	MX	10	mail2.unn.ru.

Записи о ресурсах

- NS – определяет авторизованный DNS-сервер данной зоны
 - для зоны Интернет должно быть определено не менее двух авторизованных серверов, имеющих IP-адреса в разных сетях класса C
 - для определения локальных зон можно использовать один DNS-сервер

```
unn.ru IN NS ns.unn.ru.  
unn.ru IN NS ns2.unn.ru.  
unn.ru IN NS ns3.unn.ru.
```

Записи о ресурсах

- SOA (Start Of Authority) – содержится в начале файла зоны и определяет следующие ее параметры
 - Owner, TTL, Class, Type
 - Authoritative server – основной авторизованный сервер для данной зоны
 - Responsible person – почтовый адрес администратора, ответственного за данную зону
 - Serial number – порядковый номер версии зоны (дополнительные DNS-сервера, обслуживающие зону, при обновлении сравнивают номер версии в своей копии с номером версии зоны на основном сервере и выполняют обновление только в том случае, если номер их локальной копии меньше)

Записи о ресурсах

■ SOA (Start Of Authority)

- Refresh (в секундах) – интервал, с которым дополнительные сервера зоны проверяют наличие в ней изменений
- Retry (в секундах) – интервал, через который дополнительный сервер в случае неудачного завершения обслуживания запроса на передачу предпринимает следующую попытку
- Expire (в секундах) – время после последнего успешного приема зоны, в течение которого дополнительный сервер обслуживает запросы к ней
- Minimum TTL (в секундах) – TTL по умолчанию для всех записей ресурсов зоны, также используется как TTL для отрицательных ответов для зоны

Записи о ресурсах

- Описания ресурсов последовательно размещаются в файлах зон и имеют следующий синтаксис
[Owner] [TTL] [Class] Type Data
 - запись [поле] означает, что данное поле необязательно
 - Owner (владелец) – имя узла или имя домена, которому принадлежит запись ресурса
 - если имя не указано, используется имя из предыдущей записи
 - TTL (time to live) – время жизни записи в кеше ресолвера DNS или DNS-сервера (в секундах)
 - если TTL не указан, используется минимальное значение TTL из записи SOA

Записи о ресурсах

- [Owner] [TTL] [Class] Type Data
 - Class – используемый стек протоколов, для Интернета используется значение IN; другие возможные значения – CH (Chaos), HS (Hesoid)
 - по умолчанию используется значение IN
 - Type – тип записи (SOA, NS, MX, A, и т.д.)
 - Data – данные записи ресурса, содержимое зависит от типа записи (доменное имя, IP-адрес, произвольная строка и пр.)
- Комментарии начинаются с символа ";" и заканчиваются в конце строки

Записи о ресурсах

- SOA (Start Of Authority)

unn.ru. IN SOA ns.unn.ru. admin.unn.ru. (
2008083101; Serial number
3600; Refresh (1 час)
300; Retry (10 мин)
86400; Expire (1 сутки)
3600; Minimum TTL (1 час)
)

Записи о ресурсах

- SRV – позволяет определять адреса сервисов в домене, содержит поля
 - _Service – имя сервиса
 - _Protocol – имя протокола
 - Name – имя доменной записи
 - TTL, Class, SRV
 - Priority – приоритет записи (чем меньше значение, тем выше приоритет)
 - Weight – вес записи (используется для балансировки нагрузки)
 - Port – номер порта сервиса
 - Data – доменное имя хоста, на котором запущен сервис

_http._tcp.unn.ru. IN SRV 0 0 80 www.unn.ru.

_ftp._tcp.unn.ru. IN SRV 0 0 80 ftp.unn.ru.

Записи о ресурсах

- Делегирование управления поддоменом осуществляется посредством указания в зоне родительского домена авторизованного DNS-сервера для дочернего домена
- Обычно используется следующая пара записей
 - имя_поддомена IN NS имя_DNS_сервера
 - имя_DNS_сервера IN A IP_адрес_DNS_сервера

vmk.unn.ru. IN	NS	ns.vmk.unn.ru.
ns.vmk.unn.ru.	IN	A 5.6.7.8
vmk.unn.ru. IN	NS	ns2.vmk.unn.ru.
ns2.vmk.unn.ru.	IN	A 9.10.11.12

Утилита NSLOOKUP

Команды:

- **help** или ?
- **set query=**
- **exit**

Утилита `ipconfig`

- `/displaydns`
- `/flushdns`

Имена NetBIOS и служба WINS

NetBIOS

(Network Basic Input Output System –
сетевая базовая система ввода-вывода)

Протокол NetBIOS разработан в 1984 г.
для корпорации IBM как сетевое
дополнение стандартной BIOS на
компьютерах IBM PC.

Имена NetBIOS и служба WINS

Система имен NetBIOS представляет собой простое неиерархическое пространство.

Для преобразования NetBIOS-имен в IP-адреса в операционной системе Windows Server 2003 используется служба WINS – Windows Internet Naming Service (служба имен в Интернете для Windows).

Функции сервера NetBIOS-имен описаны в RFC 1001 и 1002.

Имена NetBIOS и служба WINS

- Клиенты устанавливают сеансы с серверами
 - ☐ Регистрация имени
 - ☐ Обновление имени
 - ☐ Освобождение имени
- Методы определения имен:
 - ☐ В-узел (широковещательный)
 - ☐ Р-узел (одноранговый)
 - ☐ М-узел (смешанный)
 - ☐ Н-узел (гибридный)

Протокол LLMNR

- Протокол LLMNR (Link-Local Multicast Name Resolution)
- подходит для одноранговых служб разрешения имен для устройств с IP-адресами IPv4 и IPv6

Punycode

- стандартизированный метод преобразования последовательностей Unicode-символов в так называемые ACE-последовательности (*ASCII Compatible Encoding* - кодировка, совместимая с ASCII), которые состоят только из алфавитно-цифровых символов.
- был разработан для однозначного преобразования доменных имен в последовательность ASCII-символов.

Punycode

В качестве базисных символов выступают символы латинского алфавита а - z, цифры от 0 до 9 и дефис «-»; всего 37 символов.

Алгоритм преобразования состоит из двух этапов.

1. Из исходного текста выбираются все символы, входящие в основную кодировку ASCII (коды 0-127), и переносятся подряд в закодированное слово.
 2. Если в тексте встретились не ASCII-символы, к закодированному слову добавляется дефис, и далее преобразование идёт по процедуре, описанной в RFC3492
- Примеры**

Последовательность символов	Кодировка
abcdef	abcdef
abæcdöef	abcdef-qua4k
schön	schн-7qa
ຍຈພຟດຊຸນ	22cdfh1b8fsa
☺	74h
правда	80aafi6cg

домен.рф -> xn--d1acufc.xn--p1ai
xn--d1acufc5f.xn--p1ai -> домены.рф

DNSSEC

- **DNSSEC** (*Domain Name System Security Extensions*) - набор расширений протокола DNS, позволяющих минимизировать атаки, связанные с подменой DNS-адреса при разрешении доменных имён.
- Используется криптография с открытым ключом.
- Не обеспечивается доступность данных и конфиденциальность запросов.



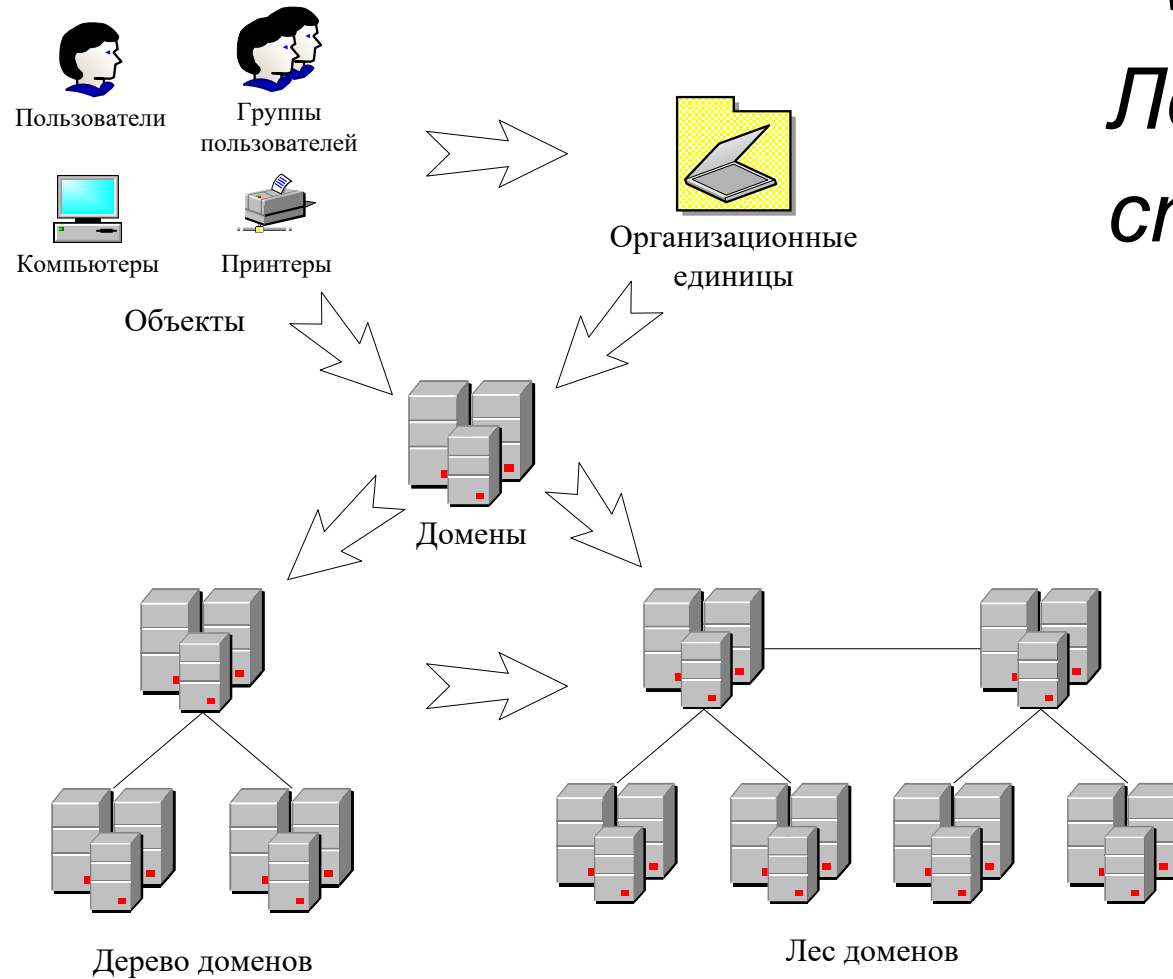
Служба каталога Active Directory

Лекция 4

План лекции

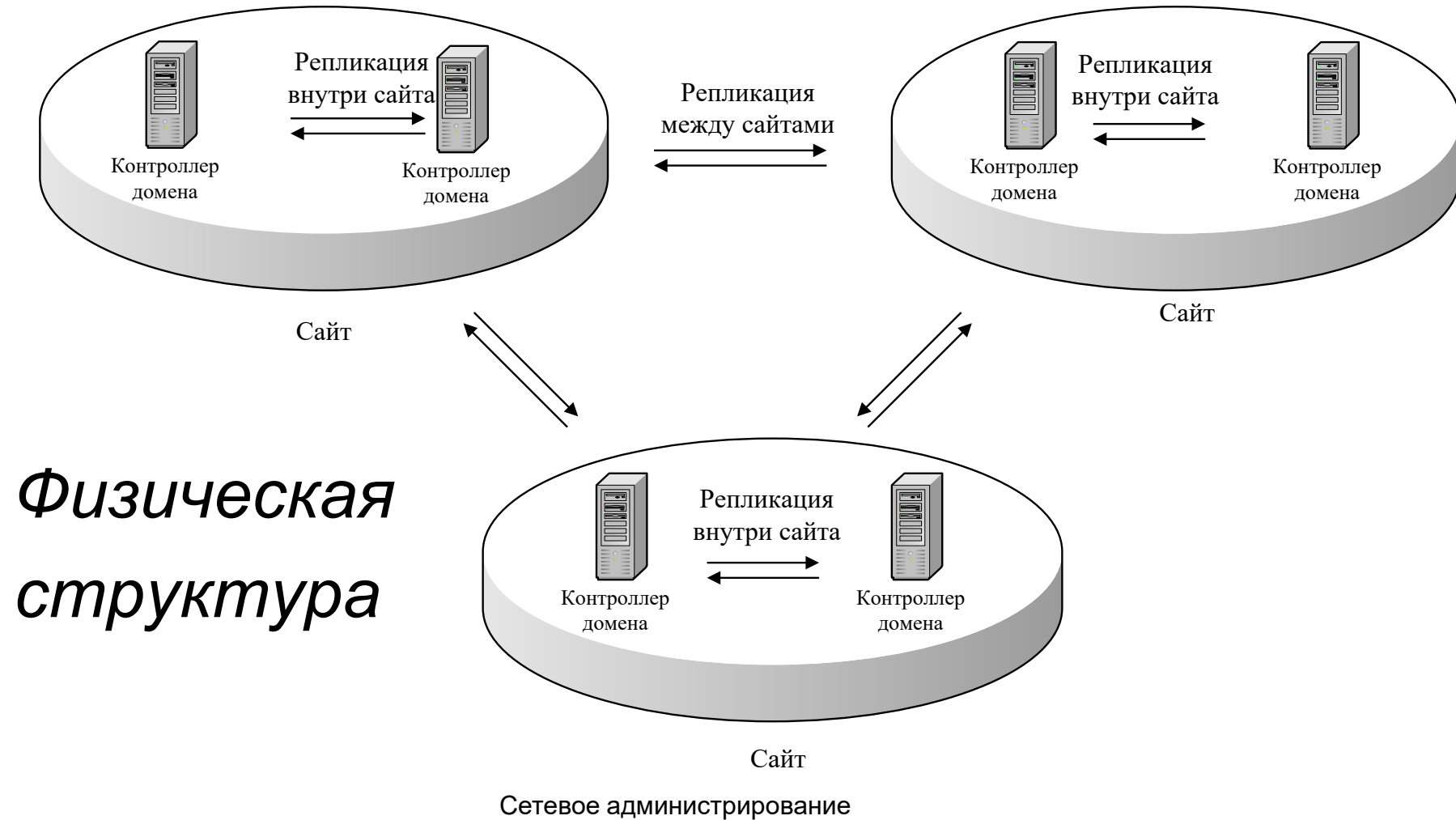
- Понятие Active Directory
- Структура каталога Active Directory
- Объекты каталога и их именование
- Иерархия доменов
- Доверительные отношения между доменами
- Организационные подразделения

Структура каталога Active Directory

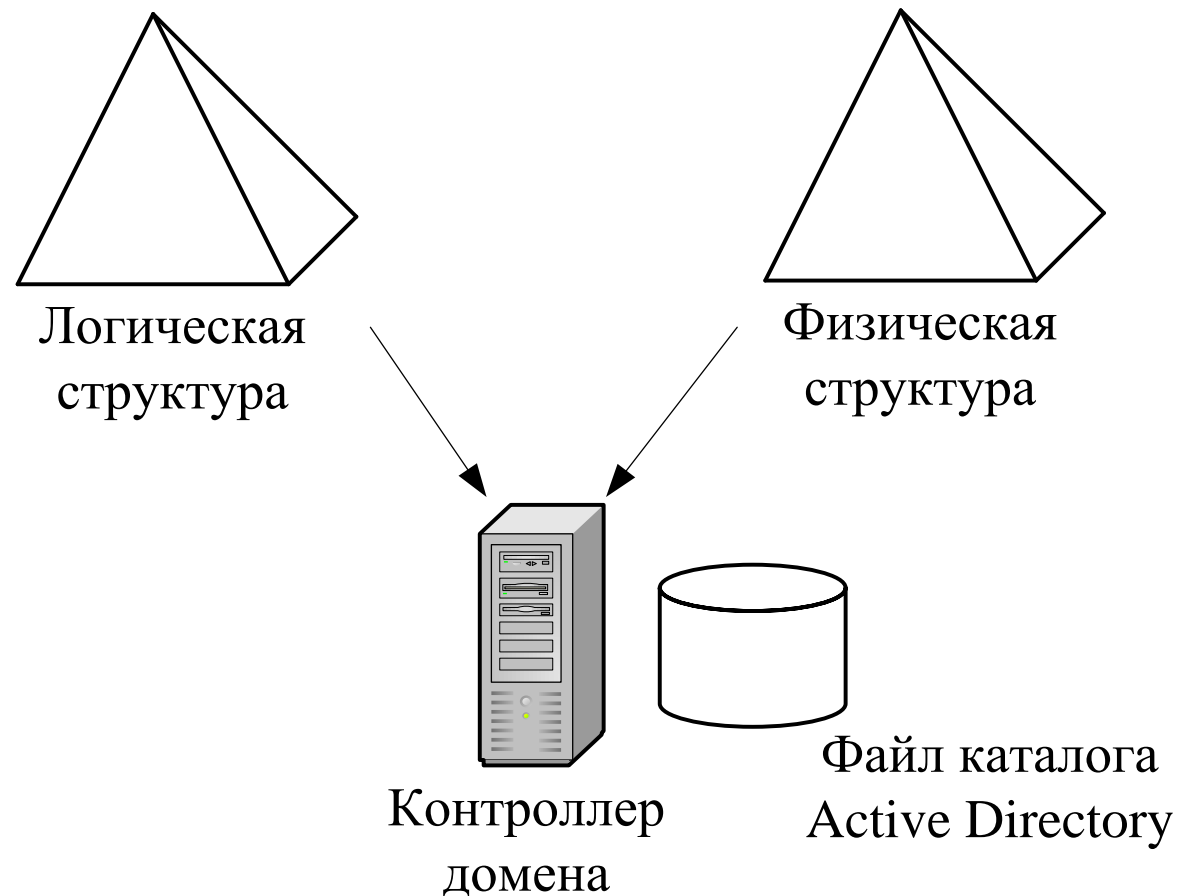


*Логическая
структура*

Структура каталога Active Directory



Структура каталога Active Directory



Структура каталога Active Directory

Ntds.dit состоит из нескольких разделов:

- *раздел домена* (domain partition)
- *раздел схемы* (schema partition)
- *раздел конфигурации* (configuration partition)
- *раздел приложений* (application partition)
- *раздел глобального каталога*
(global catalog partition)

Объекты каталога и их именование

Основные типы объектов каталога Active Directory, не являющихся контейнерами:

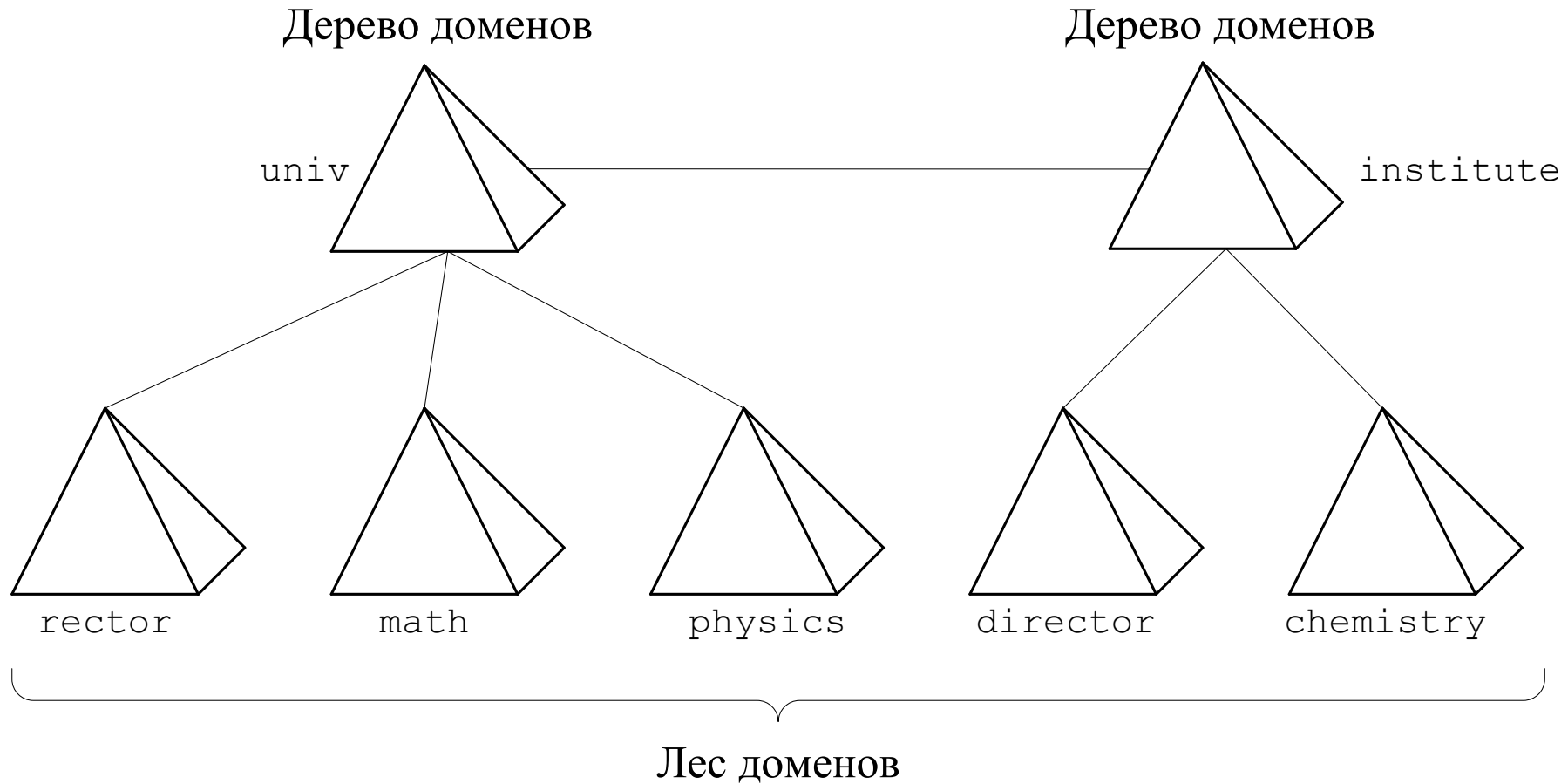
- пользователь (user)
- группы пользователей (group)
- контакты (contact)
- компьютеры (computer)
- принтеры (printer)
- общедоступные папки (shared folder)

Объекты каталога и их именование

Способы именования объектов в Active Directory:

- *Различающееся имя* (Distinguished Name, DN)
 - DC (Domain Component) – домен
 - OU (Organizational Unit) – организационное подразделение
 - CN (Common Name) – общее имя
 - Пример:
DC = ru, DC = faculty, OU = teachers, CN = users, CN = petrov
- *Относительное различающееся имя* (Relative Distinguished Name, RDN)
 - Пример: **CN = petrov**
- *Основное имя пользователя* (User Principal Name, UPN)
 - Пример: **petrov@faculty.ru**
- *Глобальный уникальный идентификатор* (Global Unique Identifier, GUID)

Иерархия доменов



Доверительные отношения

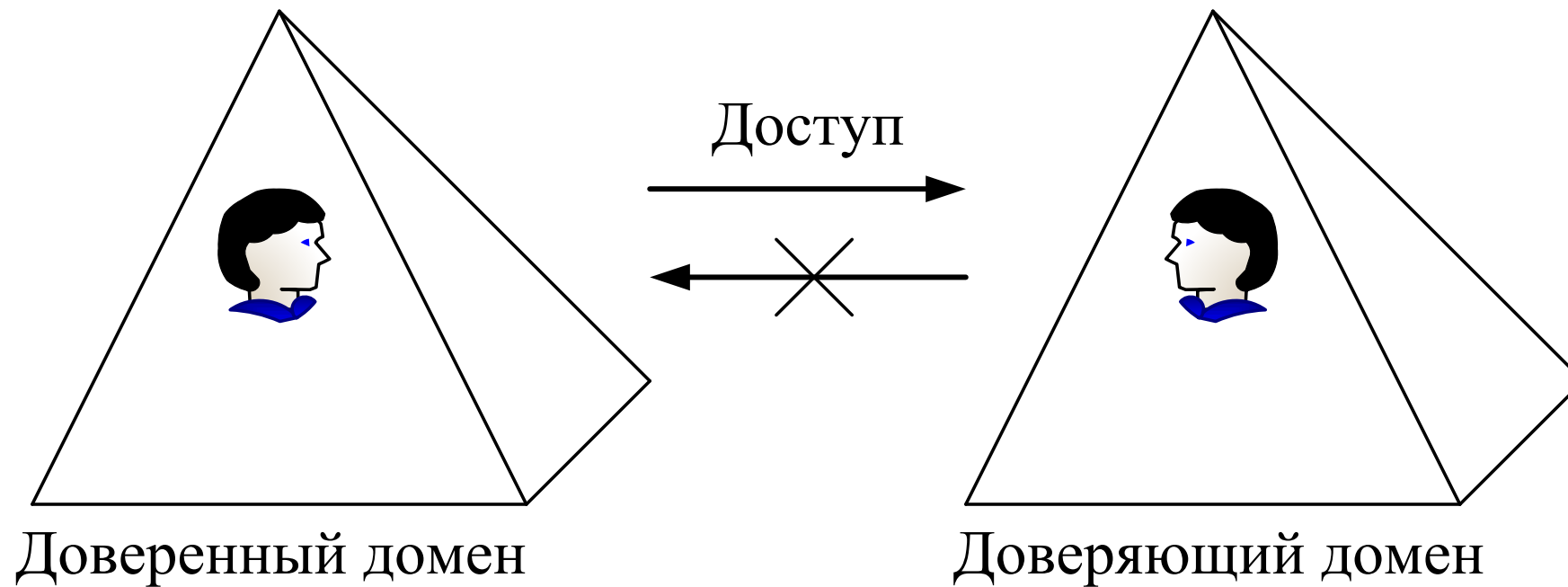
- *Аутентификация* (authentication)
- *Авторизация* (authorization)
- Для доступа к ресурсам другого домена между доменами должны быть установлены *доверительные отношения* (trust relationship).

Доверительные отношения

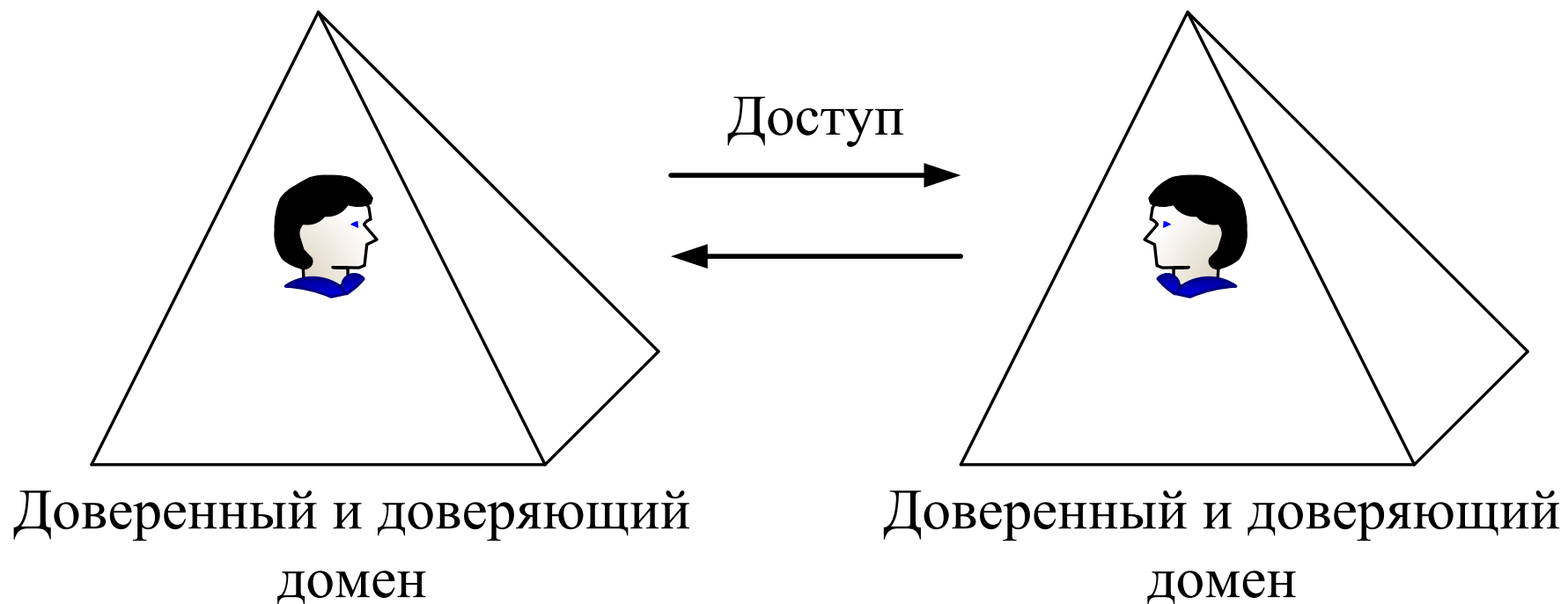
Виды доверительных отношений:

- *односторонние* (one-way trust relationship)
- *двусторонние* (two-way trust relationship) —

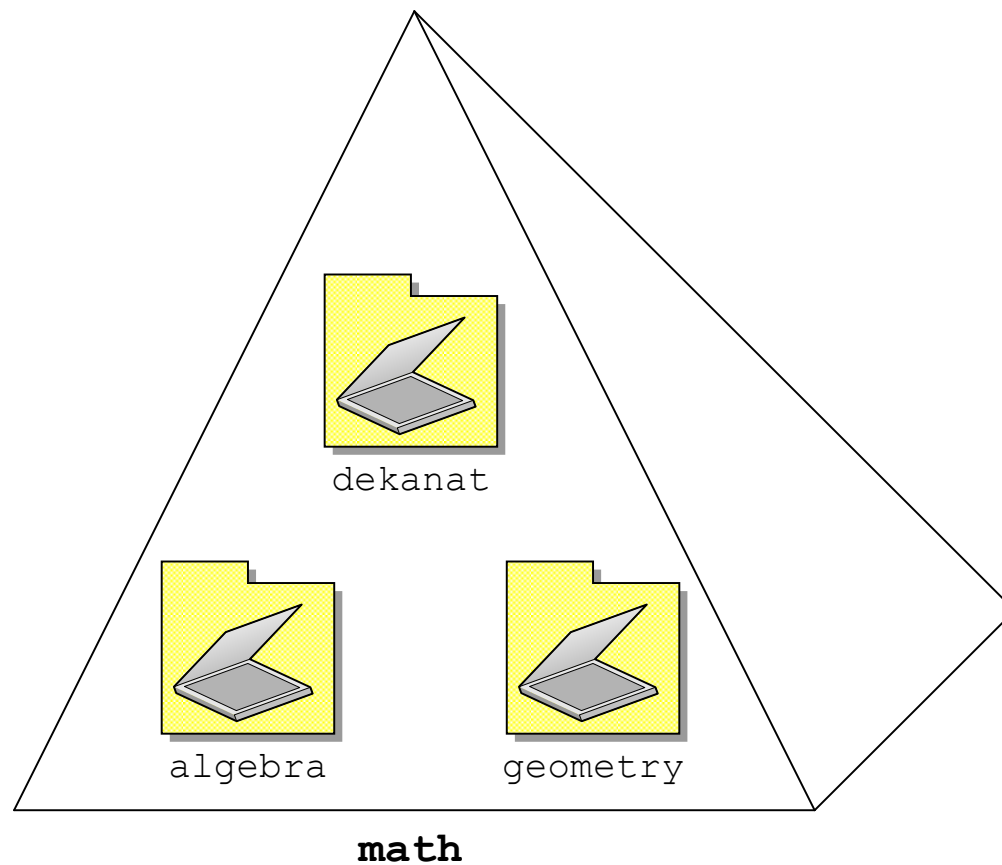
Доверительные отношения

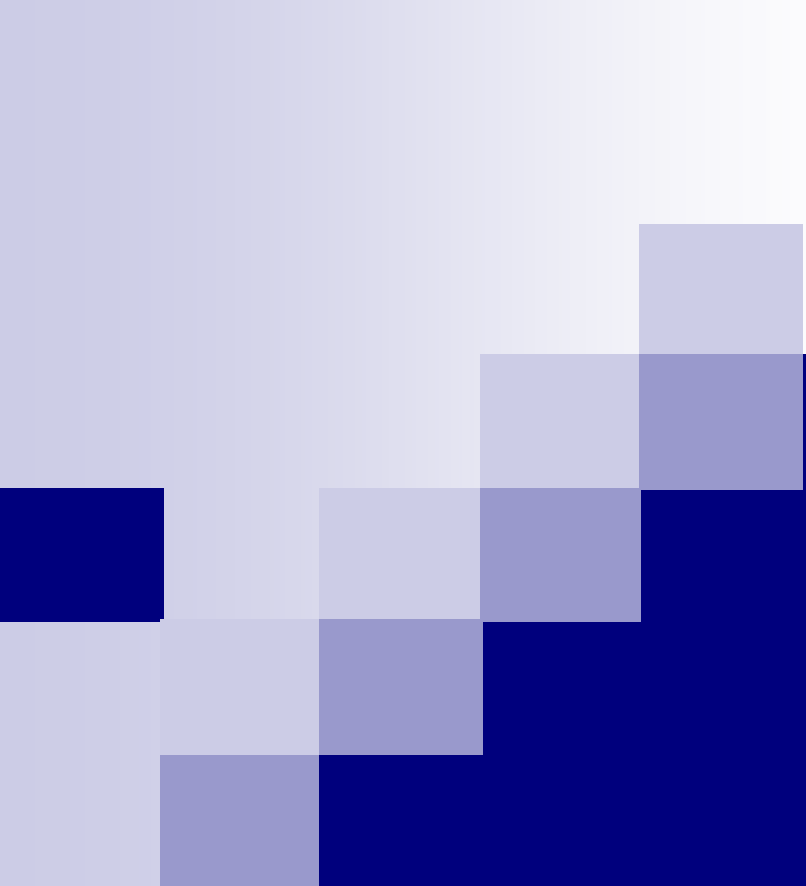


Доверительные отношения



Организационные подразделения





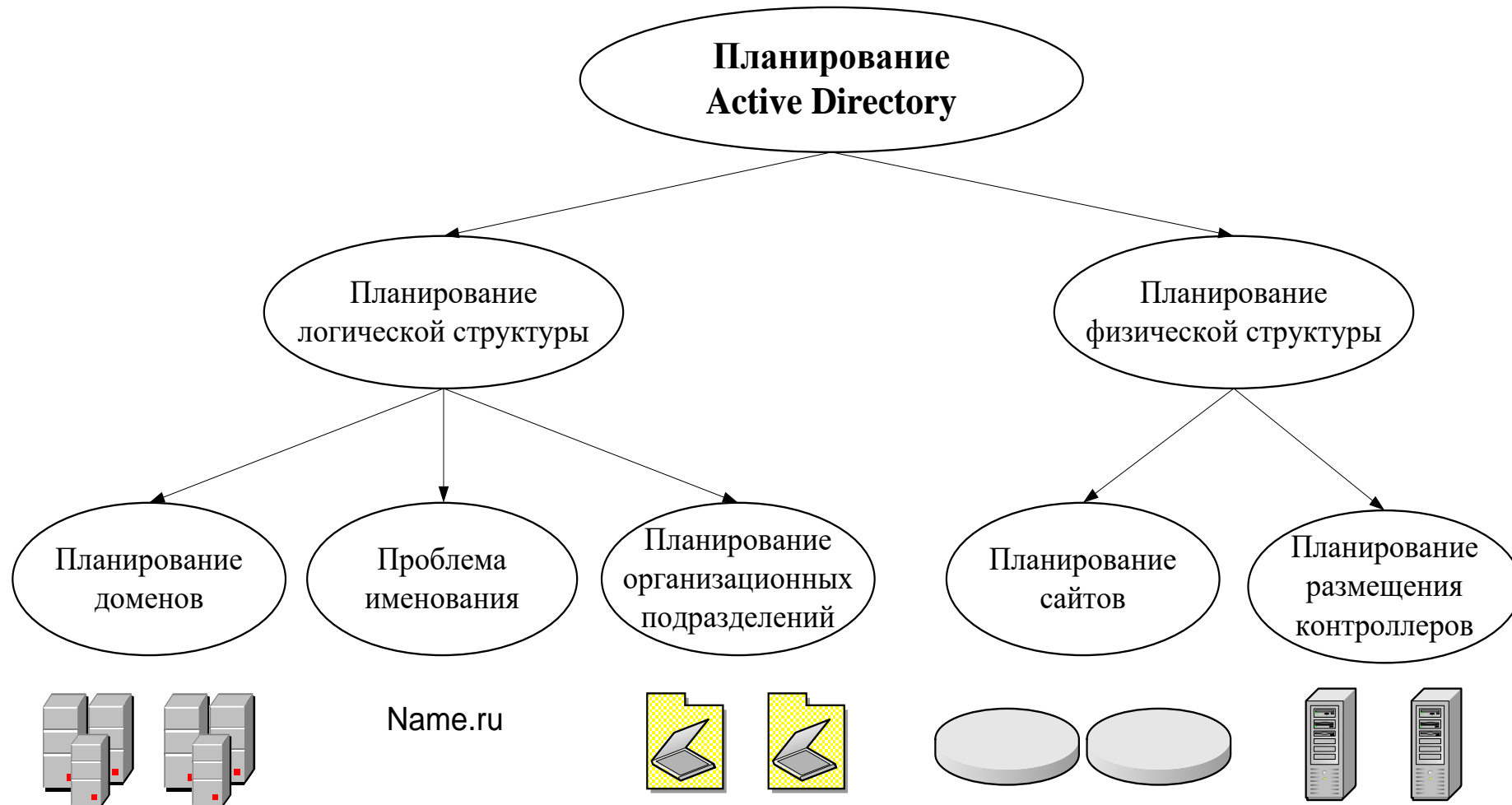
Планирование и управление Active Directory

Лекция 5

План лекции

- Планирование Active Directory
- Планирование логической структуры
- Планирование физической структуры
- Учетные записи
- Группы пользователей
- Групповые политики

Планирование Active Directory

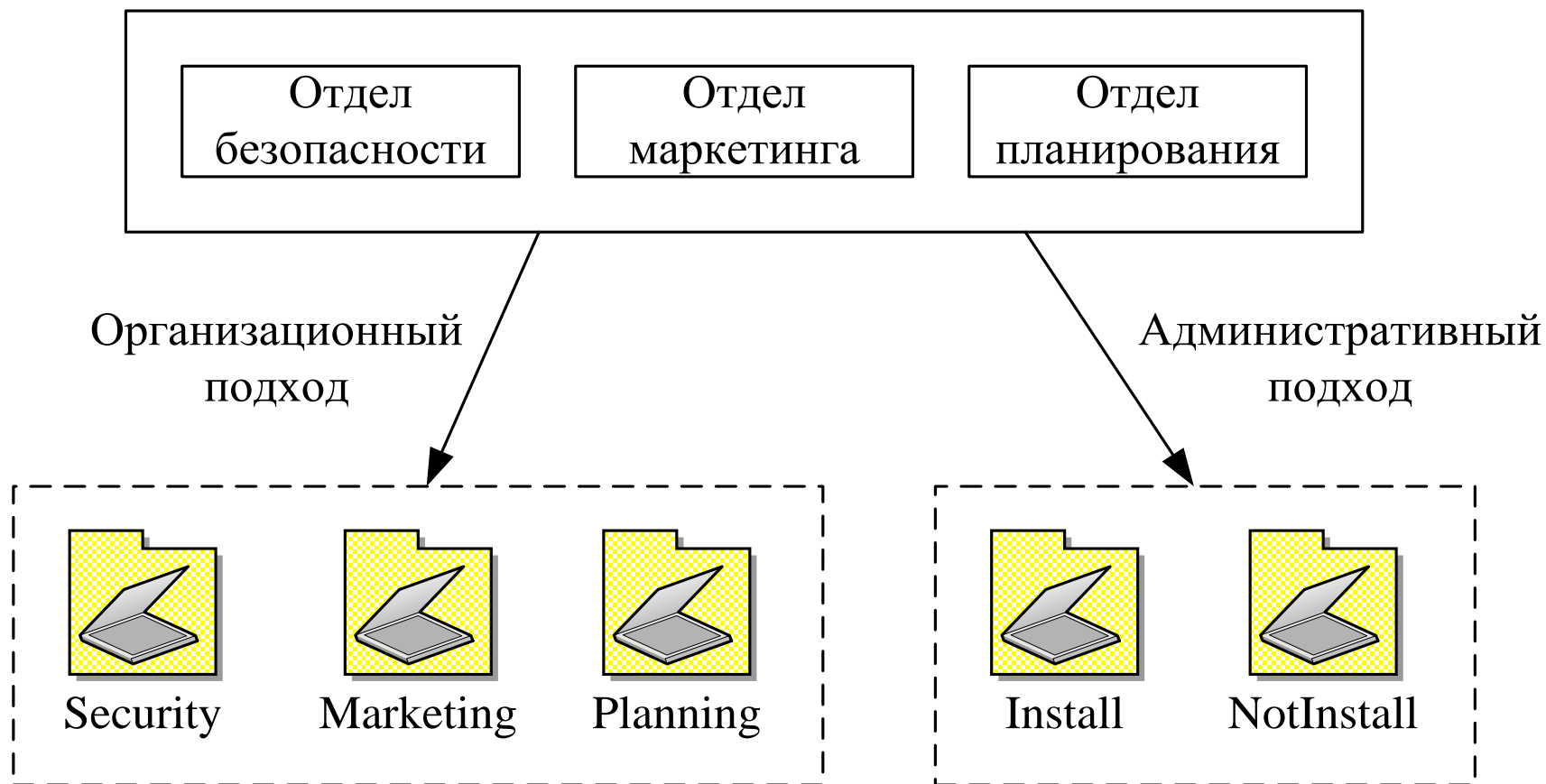


Планирование логической структуры

Признаки, по которым выбирается вариант
с одним доменом:

- в организации менее миллиона пользователей
- отсутствие удаленных филиалов
- относительная стабильность структуры организации
- отсутствие потребности в разных доменных именах
- централизованный способ администрирования
- единая политика безопасности

Планирование логической структуры



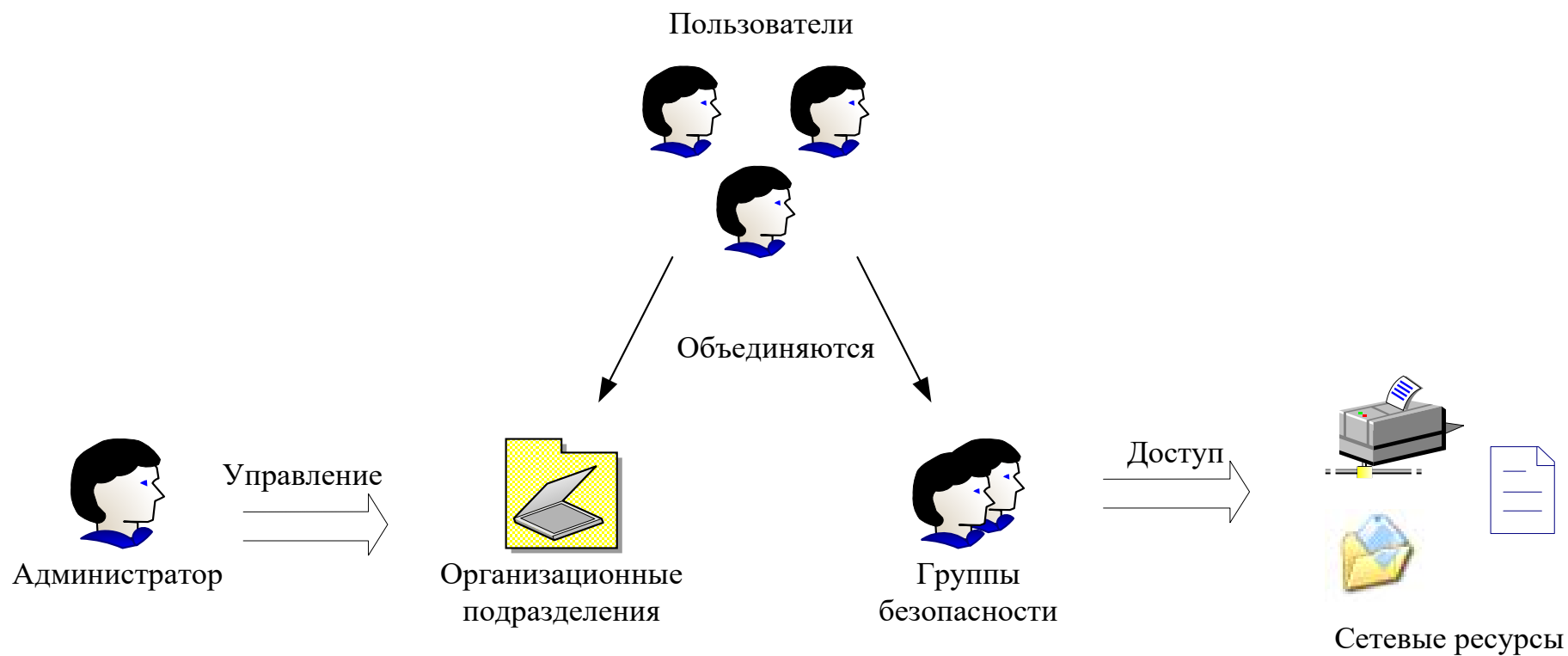
Учетные записи

Права пользователя – это список действий, которые может выполнять пользователь.

Виды прав:

- привилегия (privilege)
- право на вход в систему (logon right)
- разрешение доступа (access permission)

Группы пользователей



Группы пользователей

Области действия групп пользователей:

- доменная локальная
(domain local scope)
- глобальная (global scope)
- универсальная (universal scope)

Групповые политики

Групповые политики (group policy) – способ автоматизации работы по настройке рабочих столов пользователей и параметров компьютеров.

Групповые политики представляют собой наборы правил конфигурирования, применяемых к компьютеру или пользователю. Каждый такой набор правил называется *объектом групповой политики* (Group Policy Object, GPO).

Групповые политики

Один или несколько объектов групповой политики могут применяться к трем видам объединений:

- сайтам
- доменам
- организационным подразделениям

Для каждого компьютера может быть определен *объект локальной групповой политики* (Local Group Policy Object, LGPO).

Групповые политики

Основные части объекта групповой политики:

- **Конфигурация компьютера**
(Computer Configuration)
- **Конфигурация пользователя**
(User Configuration)

Каждая из этих частей содержит разделы:

- **Настройки приложений** (Software Settings)
- **Настройки Windows** (Windows Settings)
- **Административные шаблоны**
(Administrative Templates)



Средства обеспечения безопасности

Лекция 6

План лекции

- Средства сетевой безопасности Windows Server
- Протокол аутентификации Kerberos
- Термины, используемые в протоколе Kerberos
- Основные этапы аутентификации
- Этап регистрации клиента
- Этап получения сеансового билета
- Этап доступа к серверу
- Протокол IPsec
- Функции протокола IPsec
- Протоколы AH и ESP
- Протокол IKE

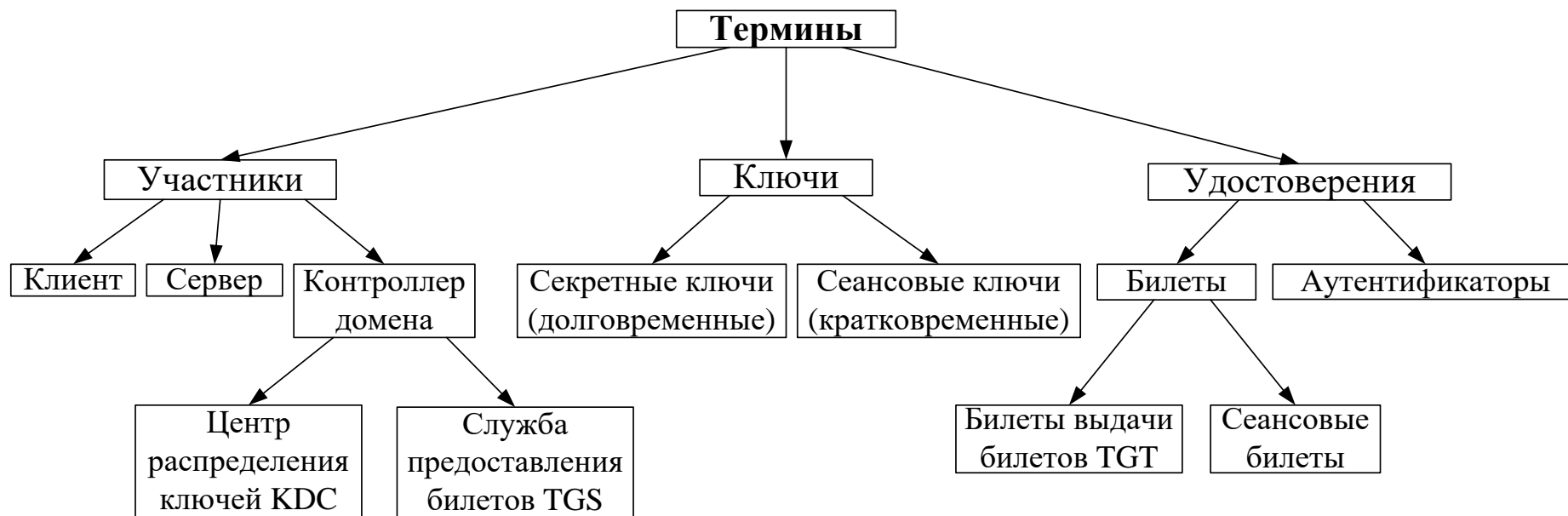
Средства сетевой безопасности Windows Server

- Основной метод аутентификации в Windows Server – протокол Kerberos v5.
- Также поддерживается протокол NTLM (NT LAN Manager).
- Для защищенной передачи сообщений наиболее надежным и перспективным считается протокол IPsec.

Протокол аутентификации Kerberos

- Начало 80-х гг., Массачусетский технологический институт (Massachusetts Institute of Technology, MIT)
- RFC 1510
- Для шифрования применяется алгоритм DES (Data Encryption Standard – стандарт шифрования данных)
-

Термины, используемые в протоколе Kerberos



Термины, используемые в протоколе Kerberos

Обозначение	Комментарий
A_C	Аутентификатор клиента
A_S	Аутентификатор сервера
K_C	Секретный ключ клиента
K_S	Секретный ключ сервера
$\{X\}K$	Сообщение X, зашифрованное ключом K
$\{A_C\}K_C$	Аутентификатор клиента, зашифрованный секретным ключом клиента

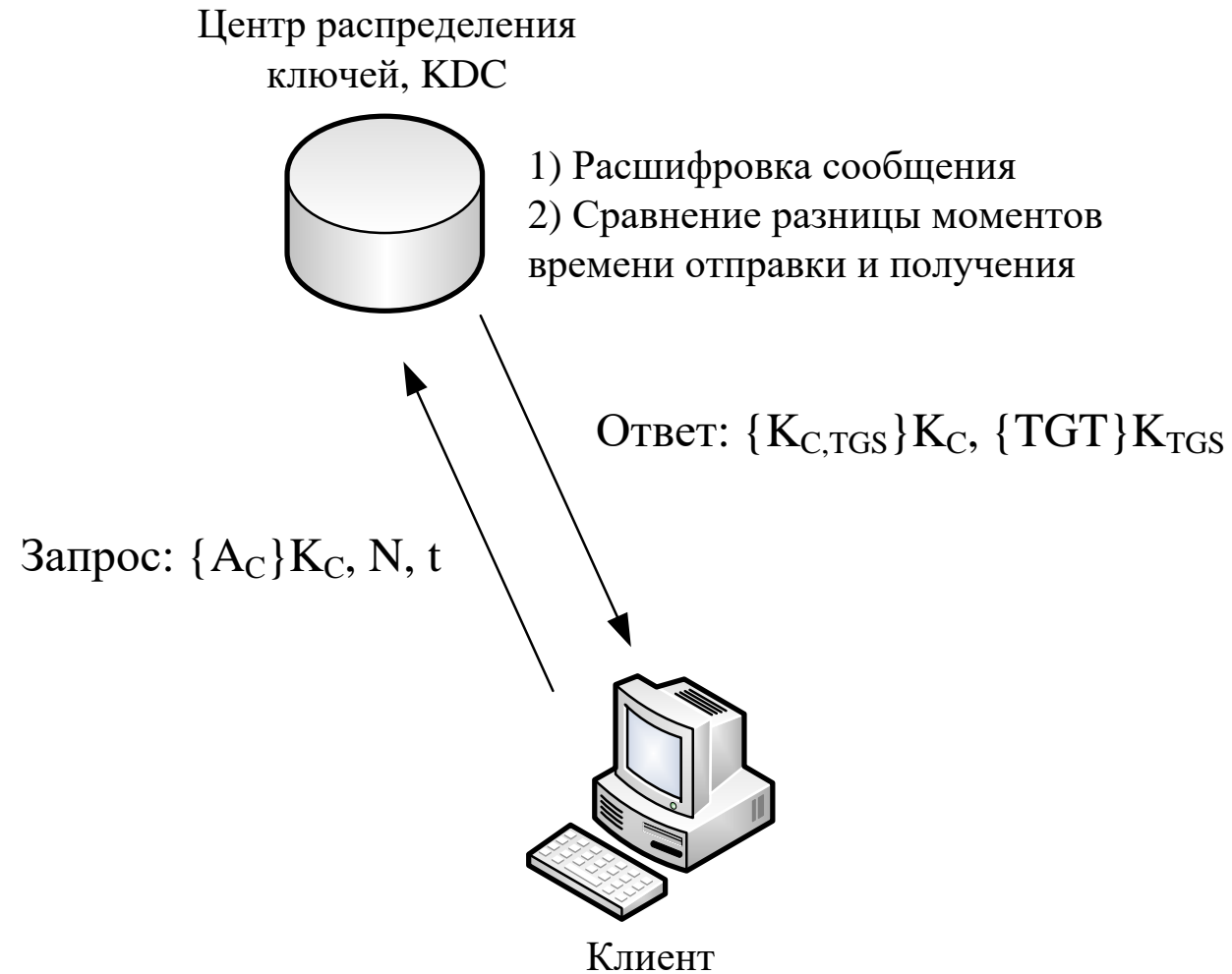
Термины, используемые в протоколе Kerberos

Обозначение	Комментарий
$K_{A,B}$	Сеансовый ключ для соединения узлов А и В
$K_{C,TGS}$	Сеансовый ключ для соединения клиента и службы TGS
TGT	Билет TGT
$T_{C,S}$	Сеансовый билет для соединения клиента и сервера
N	Имя клиента
S	Имя сервера
t	Момент времени отправки сообщения

Основные этапы аутентификации



Этап регистрации клиента



Этап получения сеансового билета

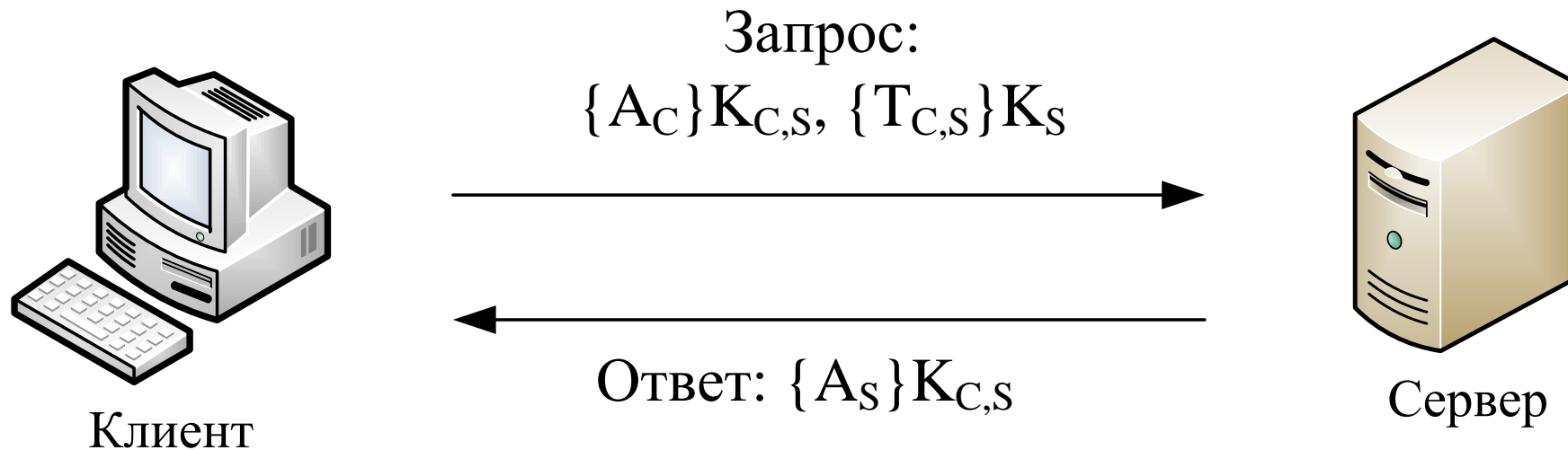


Этап получения сеансового билета

Сеансовый билет $T_{C,S}$ содержит следующие данные:

- имя сервера
- имя клиента
- сеансовый ключ
- время начала действия билета
- время окончания действия билета
- список возможных сетевых адресов клиента

Этап доступа к серверу



Средства шифрования Kerberos

- Алгоритм шифрования DES
- Используются
 - AES256-CTS-HMAC-SHA1-96
 - AES128-CTS-HMAC-SHA1-96
 - RC4-HMAC

PKINIT

В июне 2006 года был представлен [RFC 4556](#) описывающий расширение для 5-й версии под названием PKINIT

- Пользователь идентифицируется в системе и предъявляет свой закрытый ключ.
- Клиентская машина формирует запрос на СА (AS_REQ), указывает, что будет использоваться асимметричное шифрование. Запрос подписывается и, кроме стандартной информации, содержит сертификат открытого ключа пользователя.
- KDC проверяет достоверность сертификата пользователя, а затем электронную подпись. После этого KDC проверяет локальное время, присланное в запросе.
- KDC формирует ответ (AS_REP), в котором сеансовый ключ зашифровывается открытым ключом пользователя. Кроме того, ответ содержит сертификат KDC и подписывается его закрытым ключом.
- Получив ответ, пользователь проверяет подпись KDC и расшифровывает свой сеансовый ключ.

Протокол IPsec

- 1994 г., Совет по архитектуре Интернета (Internet Architecture Board, IAB), RFC 1636 «*Report of IAB Workshop on Security in the Internet Architecture*» – «Отчет семинара IAB по безопасности в архитектуре Интернета»
- IPsec (IP Security – безопасность IP), RFC 2401-2412

Функции протокола IPsec

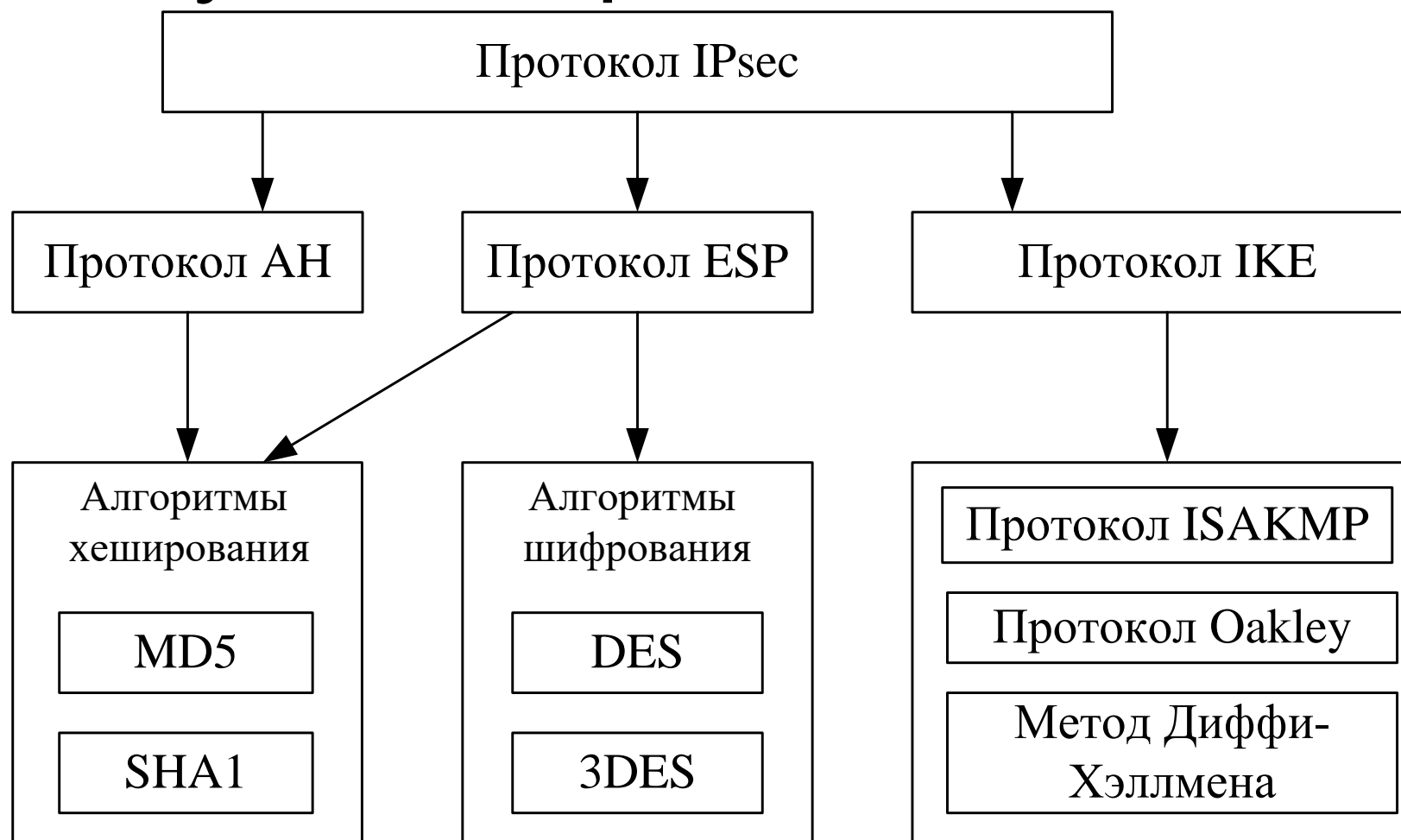
- аутентификация
- целостность
- конфиденциальность
- распределение секретных ключей

Функции протокола IPsec

Основные протоколы:

- AH (Authentication Header
– заголовок аутентификации)
- ESP (Encapsulating Security Payload
– инкапсуляция зашифрованных данных)
- IKE (Internet Key Exchange
– обмен ключами Интернета)

Функции протокола IPsec



Протоколы AH и ESP

Протокол AH (RFC 2402) снабжает пакет IPsec своим незашифрованным заголовком, который обеспечивает:

- ☐ аутентификацию исходных данных
- ☐ целостность данных
- ☐ защиту от дублирования уже полученных данных

Протоколы AH и ESP

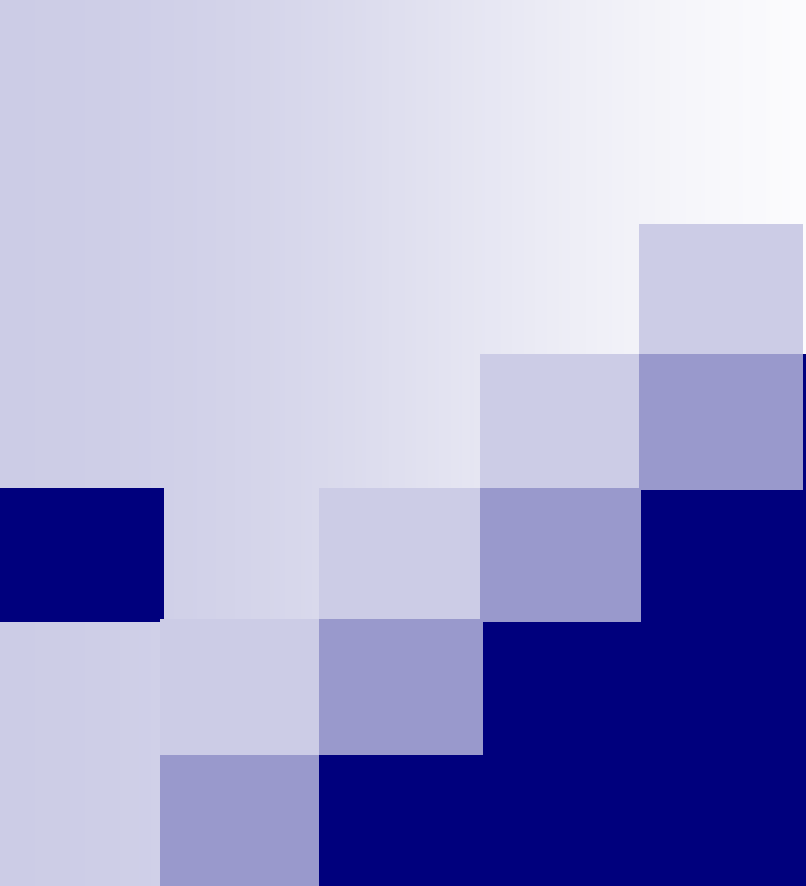
Задачи протокола ESP (RFC 2406):

- обеспечение аутентификации и целостности исходных данных
- защита от дублирования пакетов
- предоставление средств обеспечения конфиденциальности данных при помощи алгоритмов шифрования (DES и 3DES)

Протокол IKE

Протокол IKE (RFC 2409) основан на двух протоколах:

- ISAKMP (Internet Security Association and Key Management Protocol – протокол межсетевой ассоциации защиты и управления ключами)
- протокол определения ключей Оакли (Oakley Key Determination Protocol), RFC 2412, метод обмена ключами Диффи-Хэллмена (Diffie-Hellman)



Удаленный доступ и виртуальные частные сети

Лекция 7

План лекции

- Удаленный доступ
- Виды коммутируемых линий
- Протоколы удаленного доступа
- Протоколы аутентификации
- Основные понятия и виды виртуальных частных сетей
- Протоколы виртуальных частных сетей
- Протокол RADIUS

Удаленный доступ

Виды удаленного доступа:

- соединение по коммутируемой линии (dial-up connection)
- соединение с использованием виртуальных частных сетей
(Virtual Private Networks, VPN)

Удаленный доступ

- *Клиент удаленного доступа*
- *Сервер удаленного доступа*
(Remote Access Server, RAS)
- *Служба маршрутизации и удаленного доступа*
(Routing and Remote Access Service, RRAS)

Виды коммутируемых линий

Коммутируемые линии:

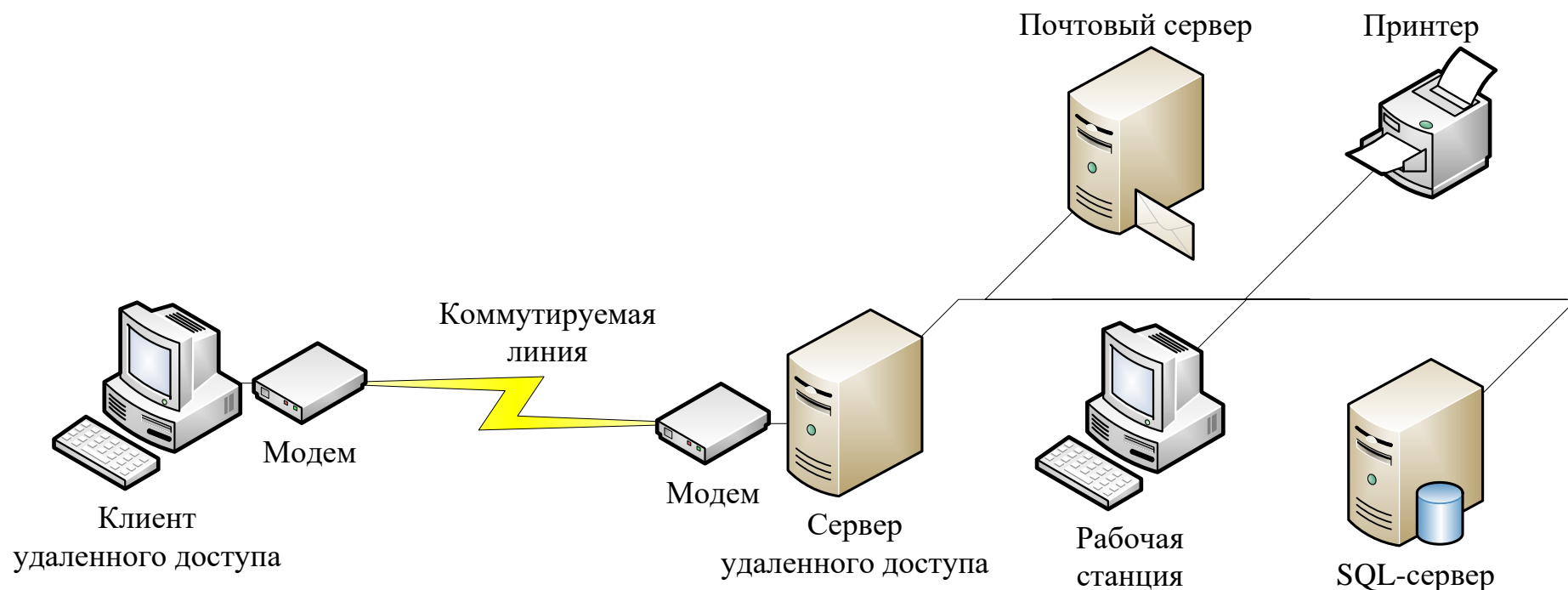
- телефонные сети: 56,6 кбит/с
- сети ISDN (Integrated Services Digital Network – цифровая сеть с комплексными услугами): 128 кбит/с
- ATM поверх ADSL – передача трафика ATM (Asynchronous Transfer Mode – асинхронный режим передачи) посредством линий ADSL (Asymmetric Digital Subscriber Line – асимметричная цифровая абонентская линия): 20 Мбит/с для входящего трафика 1 Мбит/с для исходящего трафика

Протоколы удаленного доступа

Основные этапы подключения клиента удаленного доступа:

- установка соединения
- аутентификация и авторизация клиента удаленного доступа
- сервер удаленного доступа выступает в роли маршрутизатора, предоставляя доступ клиенту к ресурсам локальной сети

Протоколы удаленного доступа



Протоколы удаленного доступа

- протокол SLIP (Serial Line Internet Protocol – межсетевой протокол для последовательного канала), RFC 1055
- протокол PPP (Point-to-Point Protocol – протокол соединения «точка-точка»), RFC 1332, 1661 и 1662

Протоколы удаленного доступа

Этапы установки соединения «точка-точка»:

1. Настройка параметров канального уровня.
2. Аутентификация клиента.
3. Обратный вызов (callback).
4. Настройка протоколов верхних уровней.

Протоколы аутентификации

- PAP (Password Authentication Protocol) – протокол аутентификации по паролю, RFC 1334
- CHAP (Challenge Handshake Authentication Protocol) – протокол аутентификации с предварительным согласованием вызова, MD-5, RFC 1994
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) – реализация протокола CHAP, разработанная Microsoft, MD-4, RFC 2433
- MS-CHAP v2 – вторая версия протокола MS-CHAP, MD-4, RFC 2759
- EAP (Extensible Authentication Protocol) – расширяемый протокол аутентификации, RFC 2284

Основные понятия и виды виртуальных частных сетей

Виртуальные частные сети (Virtual Private Network, VPN) – защищенное соединение двух узлов через открытые сети.

VPN-клиент – компьютер, инициирующий VPN-соединение.

VPN-сервер – компьютер, с которым устанавливается соединение.

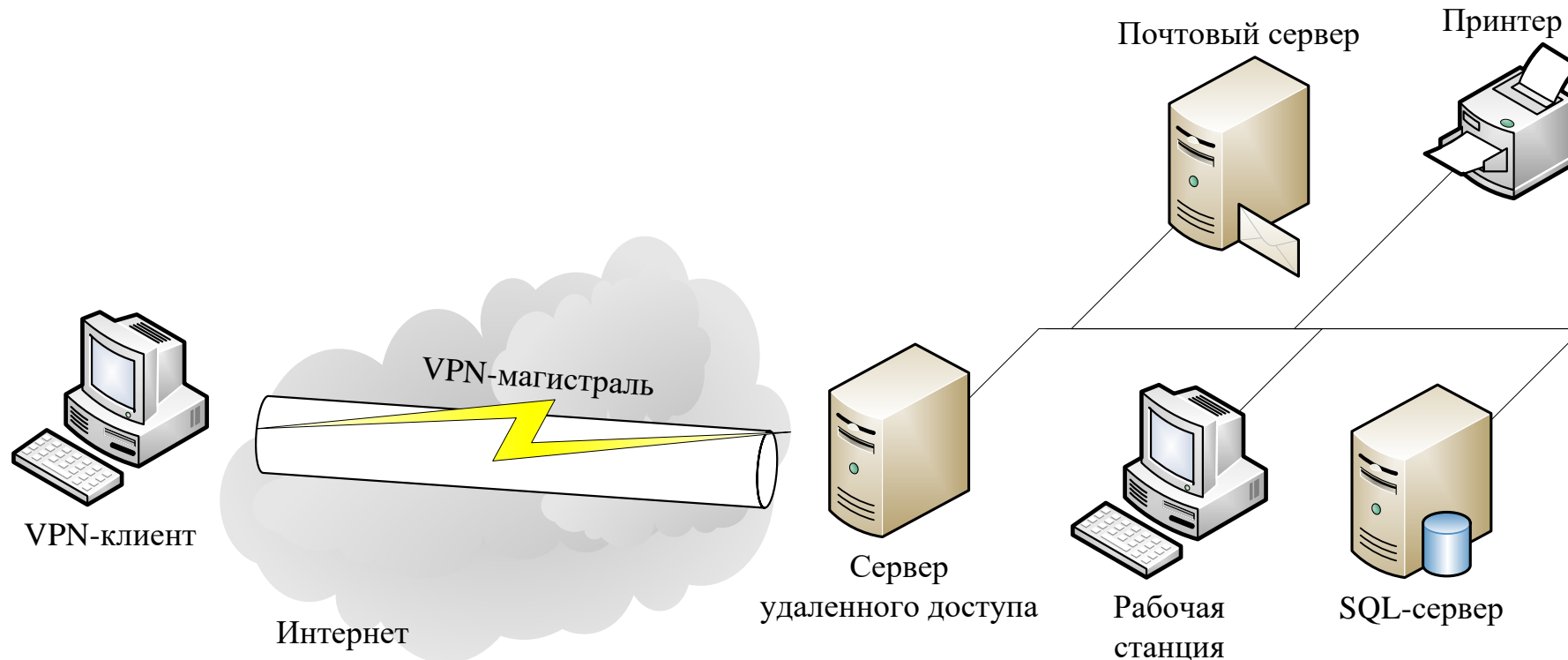
VPN-магистраль – последовательность каналов связи открытой сети, через которые проходят пакеты виртуальной частной сети.

Основные понятия и виды виртуальных частных сетей

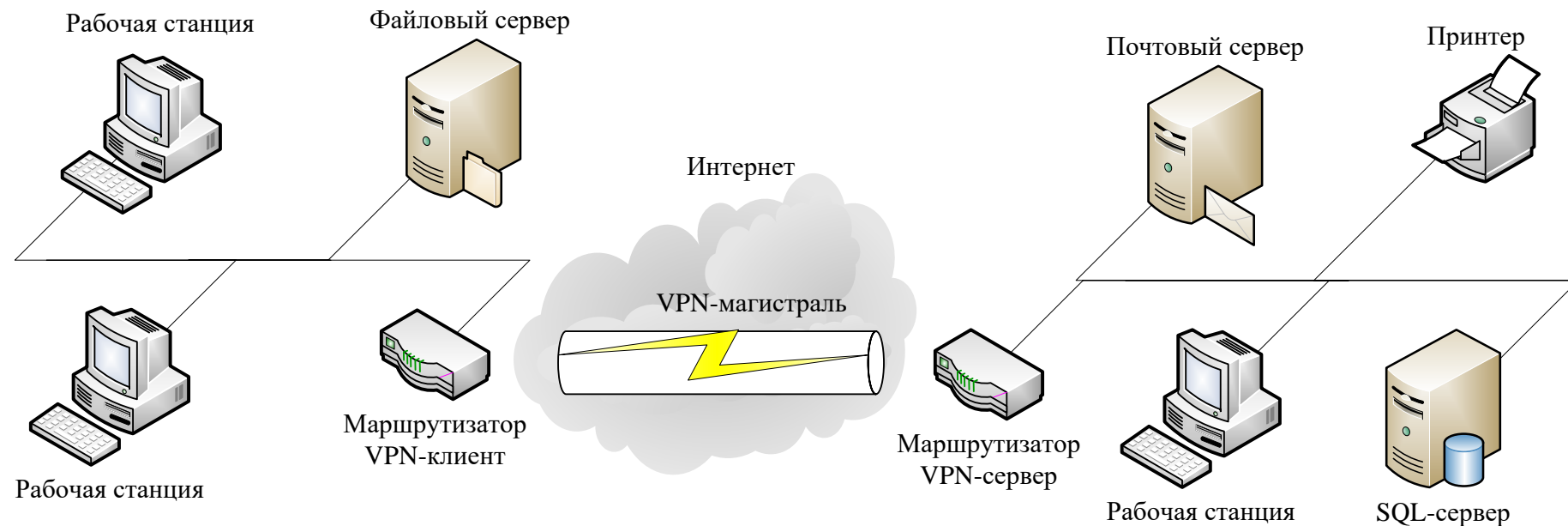
Типы VPN-соединений:

- соединение с удаленными пользователями (Remote Access VPN Connection)
- соединение маршрутизаторов (Router-to-Router VPN Connection)

Основные понятия и виды виртуальных частных сетей



Основные понятия и виды виртуальных частных сетей



Основные понятия и виды виртуальных частных сетей

VPN формируется на основе трех технологий, которые образуют защищенное соединение:

- Аутентификация
- Туннелирование
- Шифрование

Туннелирование

Туннелирование (tunneling) – процесс включения IP-пакетов в пакеты другого формата, позволяющий передавать зашифрованные данные через открытые сети.

Шифрование

Windows Server 2008 поддерживает две технологии шифрования:

- Microsoft Point-to-Point Encryption (MPPE)

- ☐ алгоритм шифрования RSA/RC4
- ☐ не сжимает данных
- ☐ используется совместно с Microsoft Point-to-Point Compression, предназначенным для этих целей
- ☐ MPPE поддерживается далеко не всеми маршрутизаторами и является частым источником несовместимости оборудования

- IPSec

- ☐ метод шифрования DES (Data Encryption Standard) или 3DES (Triple DES)
- ☐ Поддерживает сжатие данных

Протоколы виртуальных частных сетей

- PPTP (Point-to-Point Tunneling Protocol) – протокол туннелирования соединений «точка-точка», основан на протоколе PPP, RFC 2637.
 - Поддерживает все возможности PPP, в частности аутентификацию по протоколам PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP
 - Шифрование данных методом MPPE (Microsoft Point-to-Point Encryption), алгоритм RSA/RC4
 - Сжатие данных по протоколу MPPC (Microsoft Point-to-Point Compression), RFC 2118
 - Работает только поверх TCP/IP
 - Недостаток – относительно низкая скорость передачи данных

Протоколы виртуальных частных сетей

- IPsec может работать в транспортном и туннельном режимах.
 - Транспортный режим используется в связке с другими реализациями
 - туннельный сам по себе может являться методом создания VPN-туннеля.
- IPsec не создает в системе дополнительный виртуальный сетевой адаптер, а использует стандартный внешний интерфейс.
- IPsec является даже не реализацией VPN, а инструментом защиты от подмены передаваемых IP-пакетов.

Протоколы виртуальных частных сетей

- L2TP (Layer 2 Tunneling Protocol – туннельный протокол канального уровня) – протокол туннелирования, основанный на протоколе L2F (Layer 2 Forwarding) и протоколе PPTP. Описан в RFC 2661.
 - Поддерживает те же протоколы аутентификации, что и PPP
 - Шифрование данных по протоколу IPsec
 - Поддерживает сжатие данных
 - может работать поверх протоколов X.25, Frame Relay, ATM, но в системе Windows работает только поверх TCP/IP

Протоколы виртуальных частных сетей

- SSTP (Secure Socket Tunneling Protocol)
- Для защиты трафика VPN применяет протокол защищенных сокетов (SSL- Secure Socket Layer) на порте 443
- Для шифрования используется стойкий AES (до 256 бит шифрование с сертификатами до 2048-бит)

Протоколы виртуальных частных сетей

- OpenVPN – open-source реализация VPN, распространяемая под лицензией GNU GPL.
- Безопасность разворачиваемых туннелей здесь обеспечивается библиотекой OpenSSL , которая предлагает большой ассортимент открытых инструментов шифрования (Blowfish, AES, Camelia, 3DES, CAST и т.д.).
- От выбранного алгоритма зависит и скорость работы OpenVPN.
- В OpenVPN также используется инструмент LZO для сжатия данных.

Вопросы реализации VPN

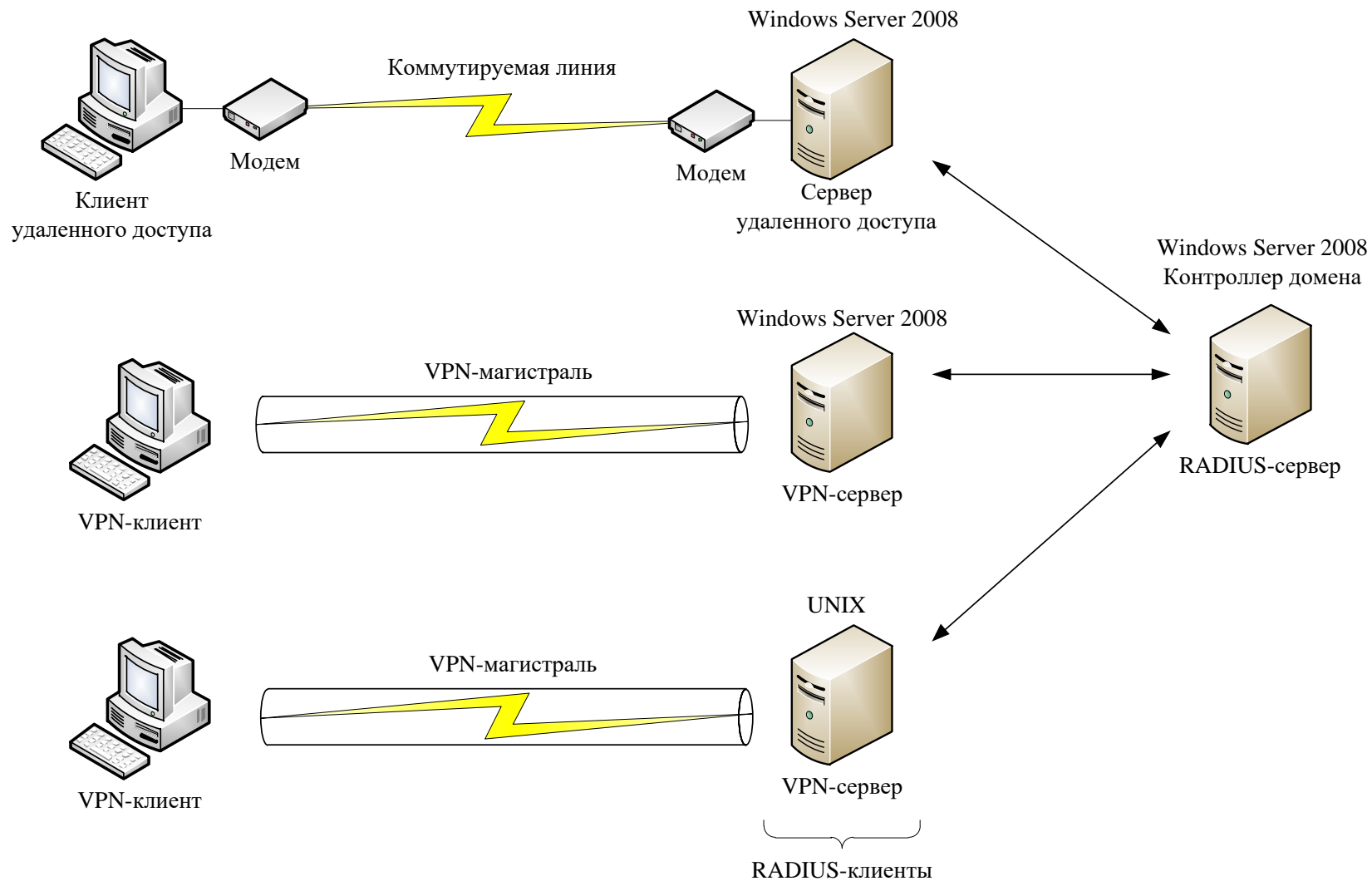
Перед реализацией VPN нужно учесть следующие факторы:

- Безопасность
- Финансовые вопросы
- Пропускная способность

Протокол RADIUS

- Протокол RADIUS (Remote Authentication Dial-In User Service – служба аутентификации пользователей удаленного доступа) предназначен для аутентификации, авторизации и учета удаленных пользователей и обеспечивает единый интерфейс для систем на разных платформах (Windows, UNIX)
- RFC 2865 и 2866
- В Windows Server 2008 протокол RADIUS входит в состав двух служб:
 - RADIUS-сервер реализуется службой Интернет-аутентификации IAS (Internet Authentication Service)
 - RADIUS-клиент можно настроить при помощи службы маршрутизации и удаленного доступа RRAS

Протокол RADIUS



Типы сообщений RADIUS

Сообщения RADIUS передаются в форме пакетов UDP.

В поле данных пакета UDP всегда помещается только одно сообщение RADIUS.

Типы сообщений RADIUS:

- Access-Request – запрос доступа
- Access-Accept – доступ разрешен
- Access-Reject – доступ не разрешен
- Access-Challenge – вызов запроса
- Accounting-Request – запрос учета

Служба IAS

