Учебный курс

Операционные среды, системы и оболочки

Лекция 14

Лекции читает

доктор технических наук, профессор

Назаров Станислав Викторович

5.7. Служба каталогов сетевых серверных ОС

5.7.1. Понятие службы каталогов

Служба каталогов (Directory Services) представляет собой базу данных и совокупность служб для именования, хранения и выборки информации в распределенной среде, доступных клиентам и администраторам этой среды.

Причины, требующие в сети централизованной базы справочной информации:

1. Появление корпоративных информационных систем. Усложнение задач управления пользователями. Централизованное хранение учетных записей пользователей.
2. Управление сетевыми ресурсами, прозрачность доступа к сетевым ресурсам.
3. Управление сетью на основе БД о топологии сети и характеристик ее компонентов. 4. Организация управления распределенными приложениями.
5. Предоставление справочной информации для работы сетевых служб и сервисов.
6. Управления качеством обслуживания сетевого трафика.

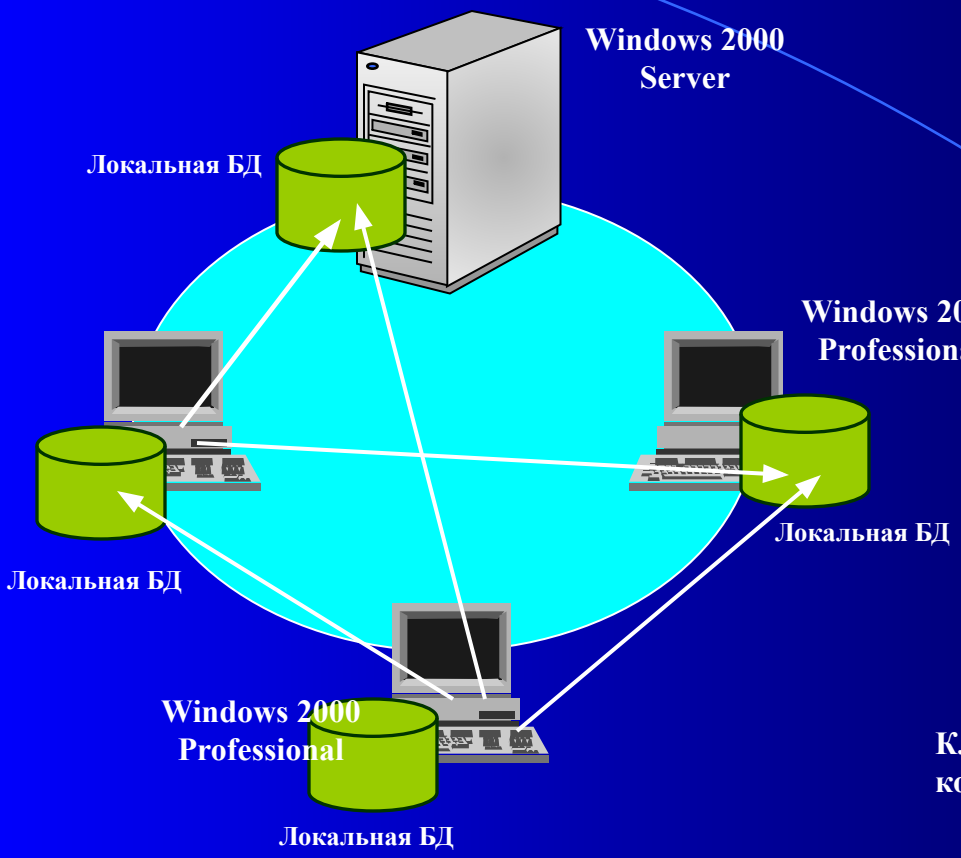
Примеры реализации службы каталогов : Novell Directory Service, Banyan Street Talk, Microsoft windows NT Directory Service, X500 (Consultative Committee for International Telephone and Telegraph, CCITT совместно с ISO).

Способы реализации:

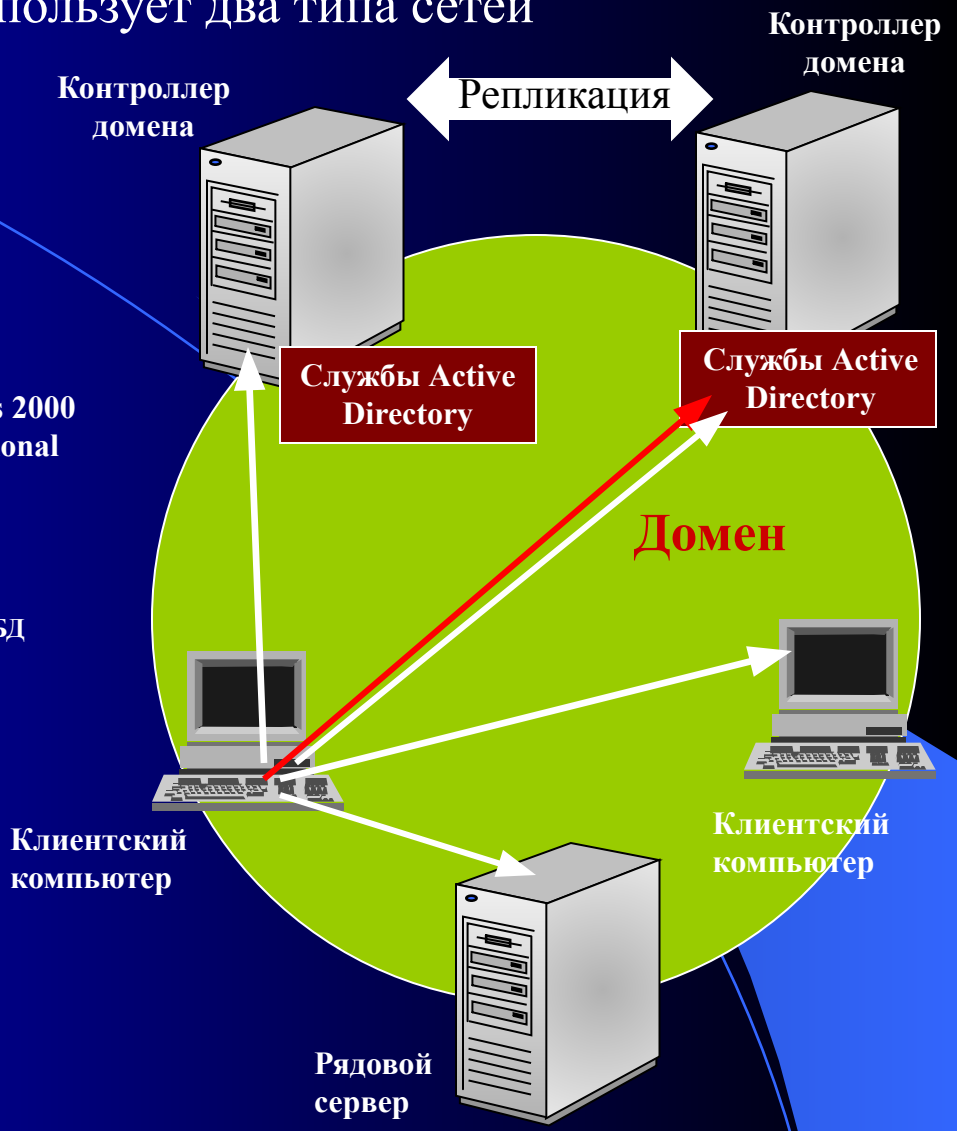
1. Локальные базы справочных служб узкого (специализированного) назначения.
2. Единая централизованная справочная служба на основе распределенной базы данных

Служба каталога использует два типа сетей

Рабочая группа



Достоинства: простота, не требуется Windows Server, удобство при небольшом количестве компьютеров при наличии опытных пользователей.



Достоинства: централизованное администрирование, однократный вход в систему, удобство работы, обеспечивают масштабирование.

5.7.2. Архитектура Active Directory

Возможности, предоставляемые службой каталогов:

- централизованное управление всеми корпоративными ресурсами;
- масштабируемость – способность охватывать домены, деревья, леса доменов;
- расширяемость каталога с возможностью добавления новых классов объектов;
- интеграция с DNS – автоматическое преобразование доменных имен в IP-адреса;
- администрирование с использованием групповых политик;
- единая регистрация в сети, доступ к ресурсам независимо от их расположения в сети;
- безопасность информации, достигаемая централизованной защитой сети;
- гибкость изменений в структуре каталога в соответствии с изменениями в структуре предприятия;
- репликация информации по схеме со многими ведущими.

Технологии, положенные в основу архитектуры Active Directory:

1. Стандарты X500 и X509, определяющие информационную модель данных, синтаксис и формат цифровых сертификатов, используемых для аутентификации пользователей.
2. Стандартный протокол доступа к каталогам LDAP (Lightweight Directory Access Protocol).
3. Стек протоколов TCP/IP, являющийся основным в сетях масштаба корпорации.
4. Служба DNS, используемая для разрешения доменных имен в IP-адреса.
5. Протокол динамической конфигурации клиента DHCP.
6. Система Kerberos – протокол аутентификации пользователей.

DSA предоставляет API-интерфейсы для выполнения запросов доступа к каталогу.

Уровень базы данных обеспечивает объектное представление информации БД путем применения семантики схемы к записям БД и изолирования верхних уровней службы каталога от исходной СУБД реляционного типа.

Расширяемое ядро хранилища – файл базы данных Ntds.dit – обрабатывается только ядром хранилища. Администрирование этого файла осуществляется утилитой Ntdsutil .

Компоненты Active Directory

Логическая структура:

- ***объект*** **– конкретная сущность (пользователь, принтер, папка, компьютер и т.д.) с отличительным набором атрибутов;**
- ***контейнер*** **– логическое объединение, группирующее объекты или контейнеры по некоторому признаку;**
- ***организационное подразделение*** **– некоторый контейнерный объект, организующий объекты в логические административные группы;**
- ***домен*** **– группа компьютеров, совместно использующих общую БД каталога;**
- ***дерево доменов*** **–группировка одного или нескольких доменов со смежной структурой имен, предоставляющая совместный доступ к ресурсам;**
- ***лес доменов*** **– объединение одного или более деревьев совместно использующих информацию каталога.**

Физическая структура:

- ***контроллер домена*** **– компьютер с серверной ОС Windows Server, хранящий раздел каталога (локальную БД домена) и отвечающий за аутентификацию пользователей;**
- ***подсеть*** **– сетевая группа с заданной областью IP-адресов и сетевой маской, которая имеет определенное географическое положение;**
- ***сайт*** **– одна или несколько подсетей со своим множеством IP-адресов.**

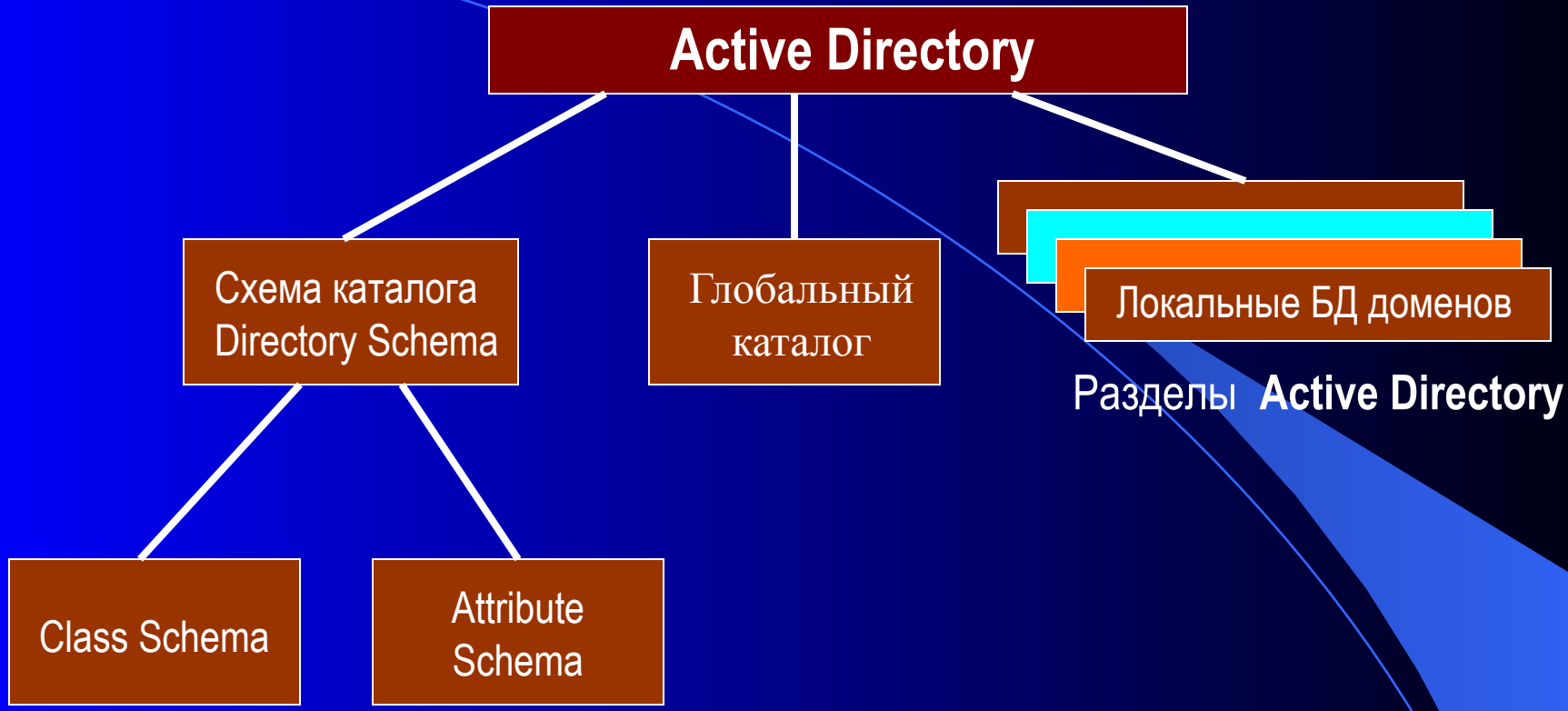


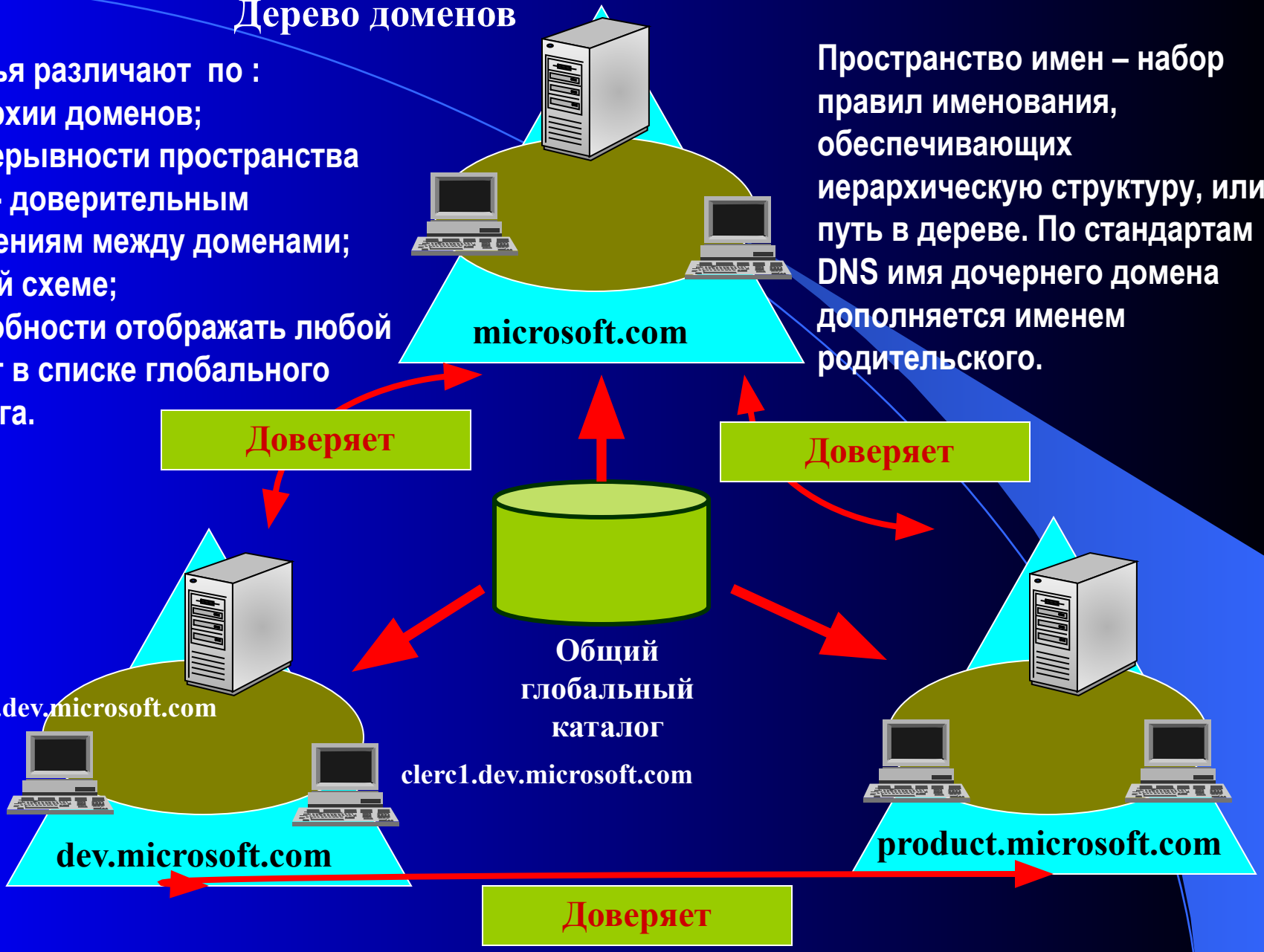
Схема каталога – определения всех объектов и правила, описывающие структуру каталога, синтаксис объектных классов и типы атрибутов, входящих в каталог.

Сеть корпоративного предприятия представляется доменным деревом или доменным лесом.

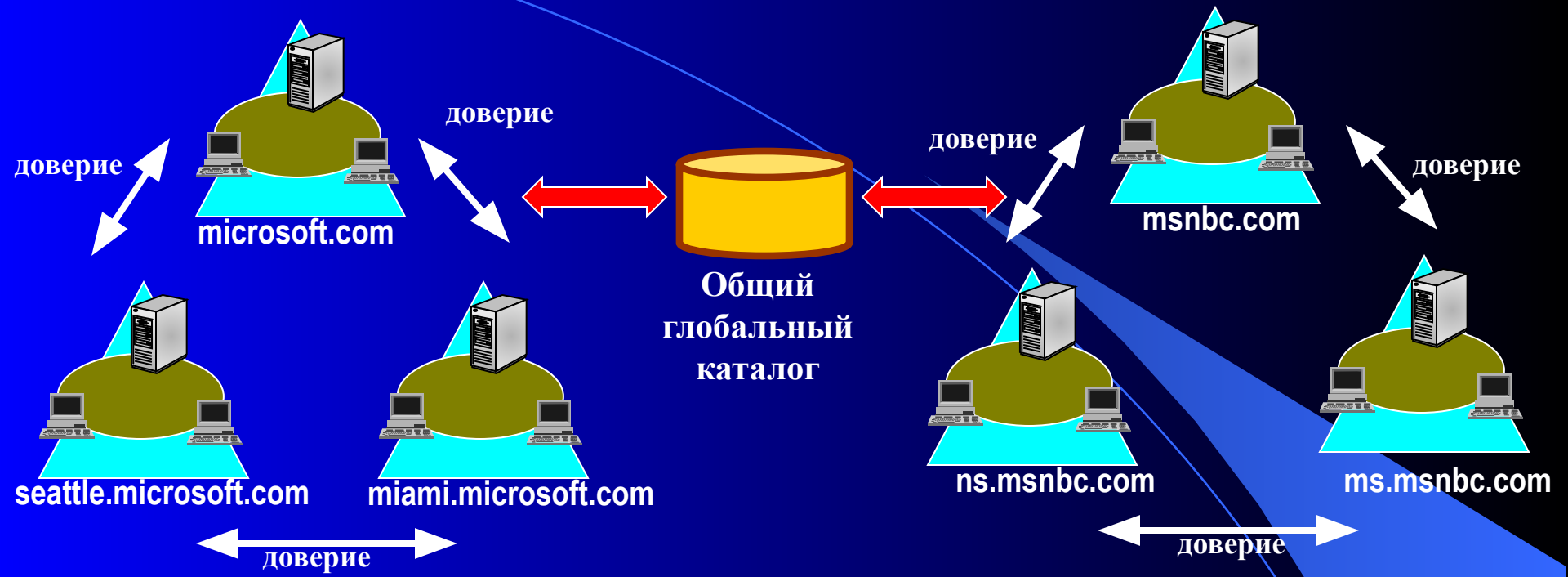
Дерево доменов

Деревья различают по :
- иерархии доменов;
- непрерывности пространства имен; - доверительным отношениям между доменами;
- общей схеме;
- способности отображать любой объект в списке глобального каталога.

Пространство имен – набор правил именования, обеспечивающих иерархическую структуру, или путь в дереве. По стандартам DNS имя дочернего домена дополняется именем родительского.



Лес доменов

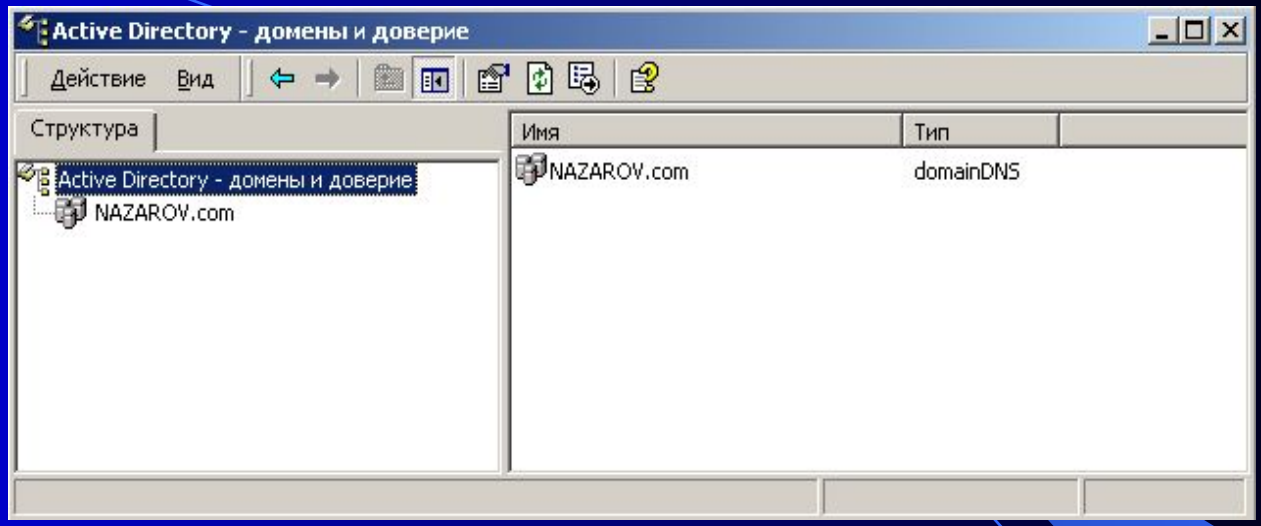


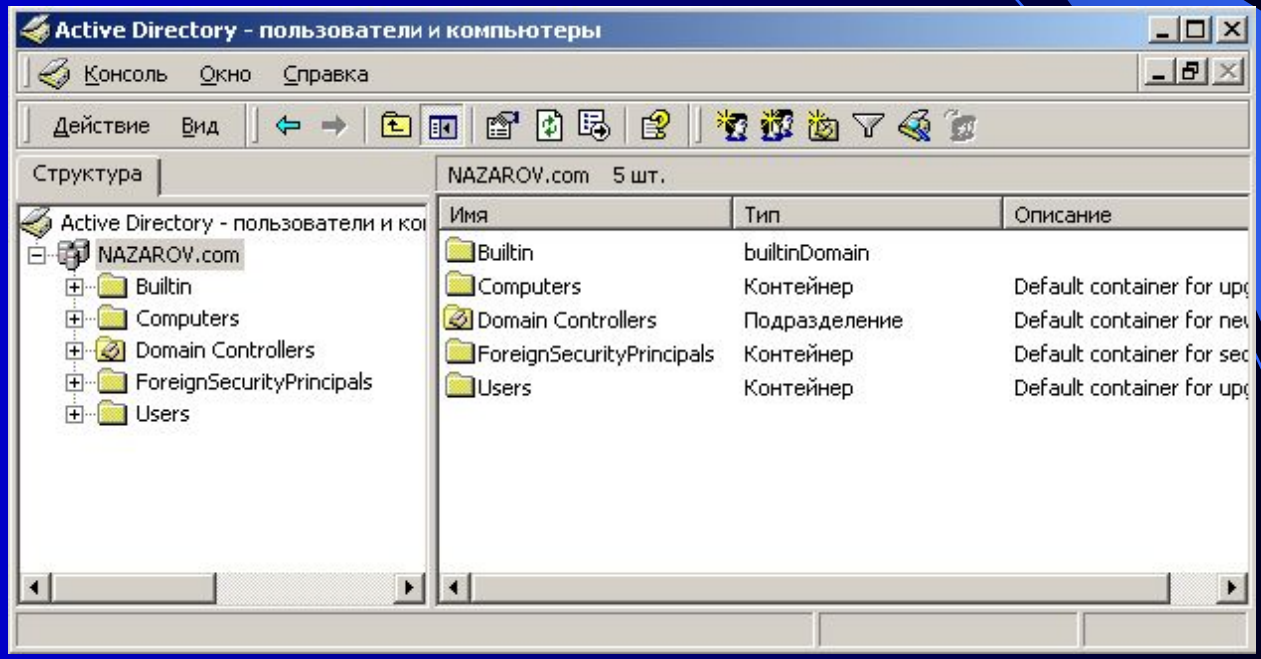
Леса различаются по:

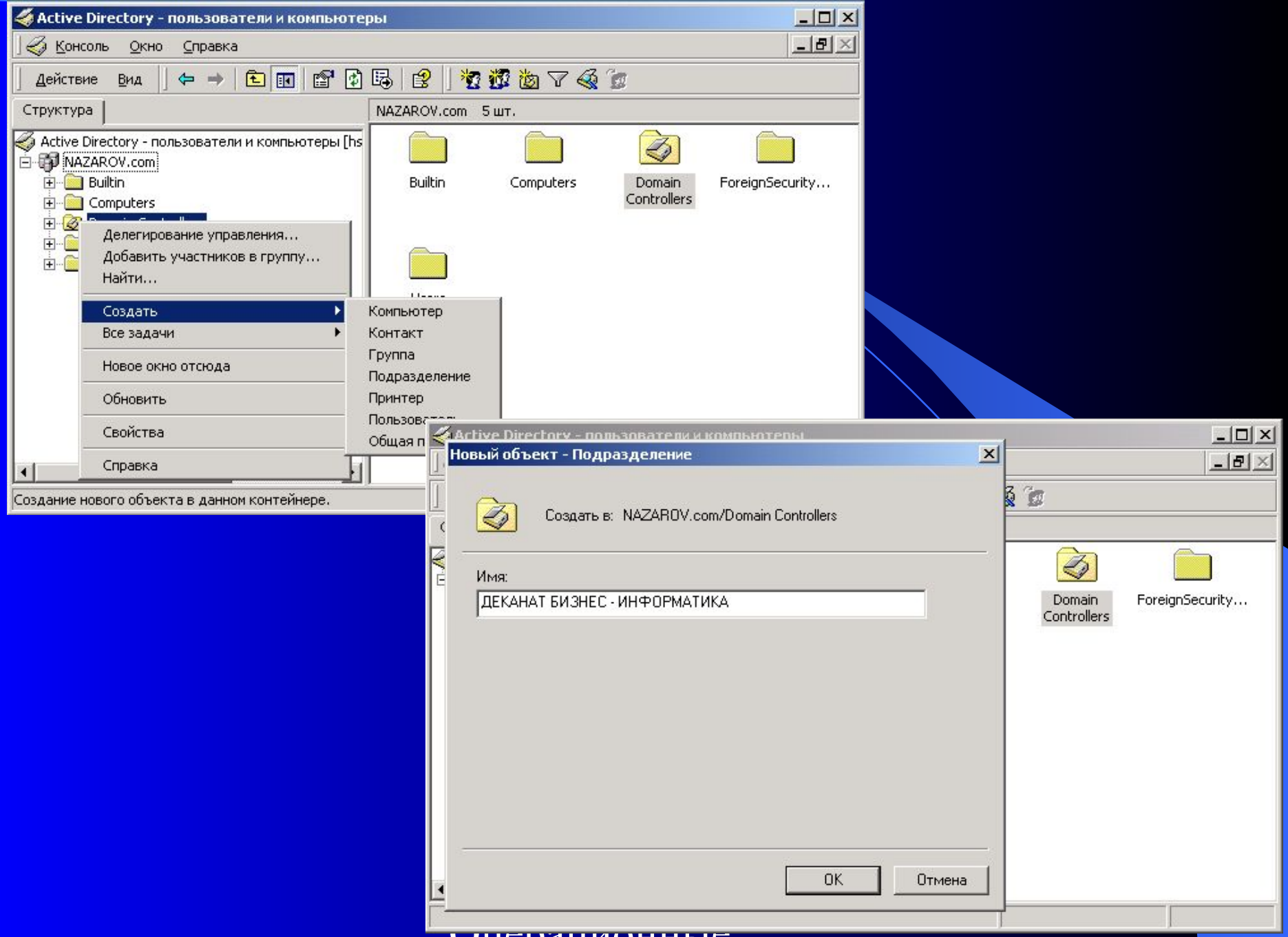
- одному или более набору деревьев;
- несвязанному пространству имен между деревьями;
- доверительным отношениям между этими деревьями;
- общей схеме;
- способности отображать любой объект в списке глобального каталога.

Доверительные отношения: - односторонние (явное доверие); - двусторонние - транзитивные (полное доверие).

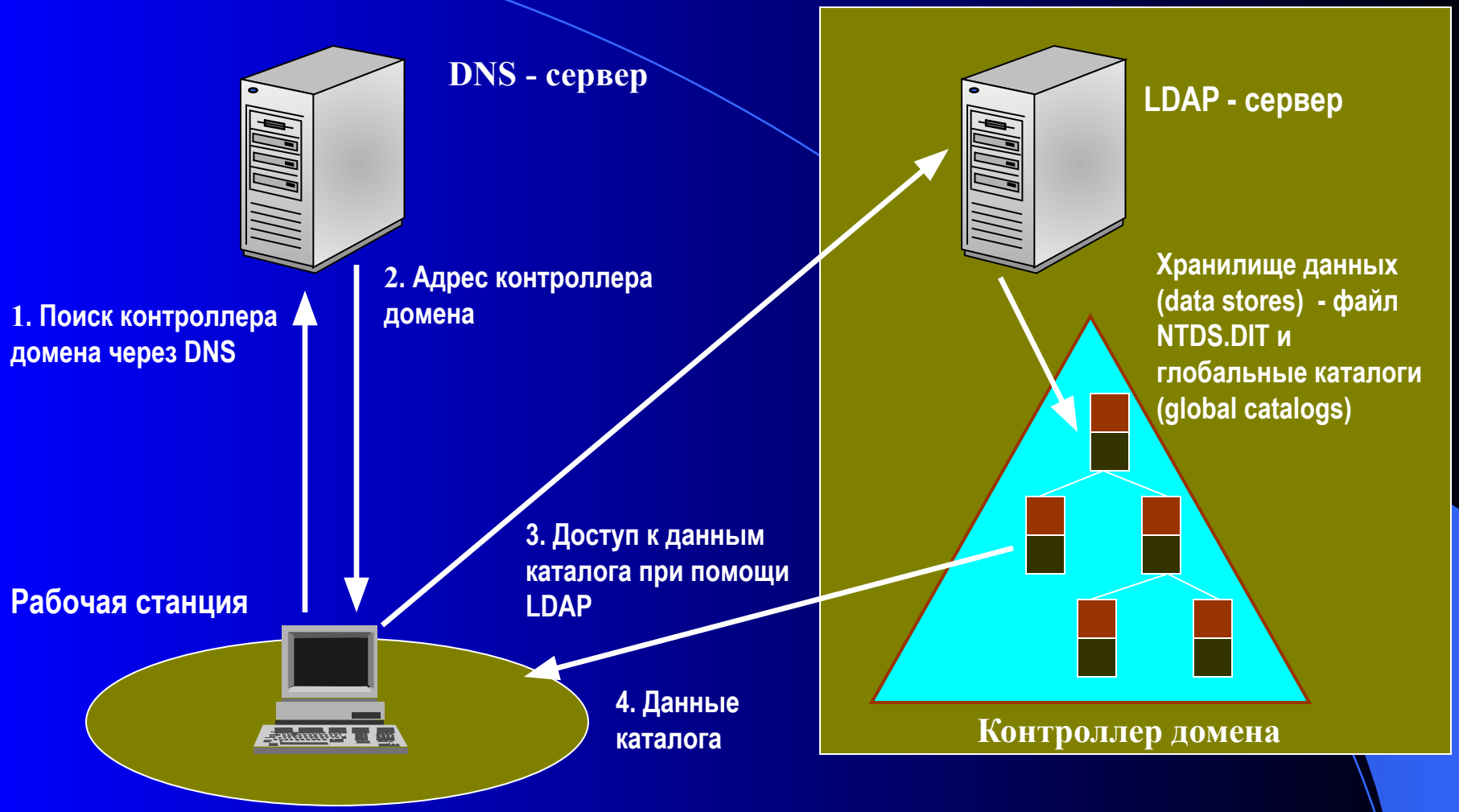
Управление доменами, ОП, пользователями и компьютерами






Active Directory - пользователи и компьютеры
Консоль Окно Справка
Действие Вид
Структура
Active Directory - пользователи и компьютеры [hs
NAZAROV.com
Builtin
Computers
NAZAROV.com 5 шт.
Builtin
Computers
Domain Controllers
ForeignSecurity...
Делегирование управления...
Добавить участников в группу...
Найти...
Создать
Все задачи
Новое окно отсюда
Обновить
Свойства
Справка
Компьютер
Контакт
Группа
Подразделение
Принтер
Создание нового объекта в данном контейнере.
Новый объект - Подразделение
Создать в: NAZAROV.com/Domain Controllers
Имя:
ДЕКАНАТ БИЗНЕС - ИНФОРМАТИКА
OK
Отмена

5.7.3. Контроллеры домена и сайты



NTDS.DIT СОДЕРЖИТ: 1. Данные домена – информация об объектах домена (учетные записи, общие ресурсы, ОП, групповые политики). 2. Данные конфигурации (топология каталога, список лесов, деревьев, контроллеров и серверов ГК). 3. Данные схемы - информация об объектах и типов данных, которые могут храниться в каталоге.

Доступ и распространение данных Active Directory. Протоколы и репликация

Основной метод репликации - режим multi-master – репликация с несколькими хозяевами. Часть изменений в каталоге выполняется в режиме с одним основным контроллером – основным контроллером операций (operations master – хозяин операций). Роли контроллера операций FSMO (Flexible Single Master Operation – гибкие операции с одним основным контроллером):

Хозяин схемы (Schema Master) – управляет обновлениями и изменениями схемы каталога.

Хозяин именования доменов (Domain Naming Master) – управляет добавлением и удалением доменов в лесу.

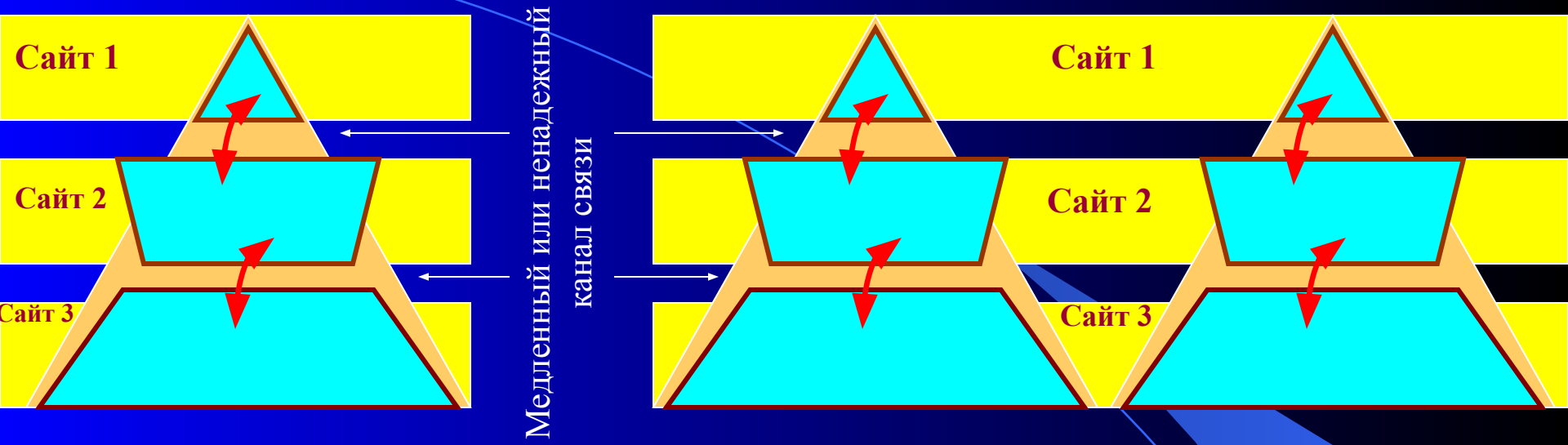
Хозяин относительных идентификаторов (RID – Relative ID Master) – выделяет относительные идентификаторы контроллерам доменов.

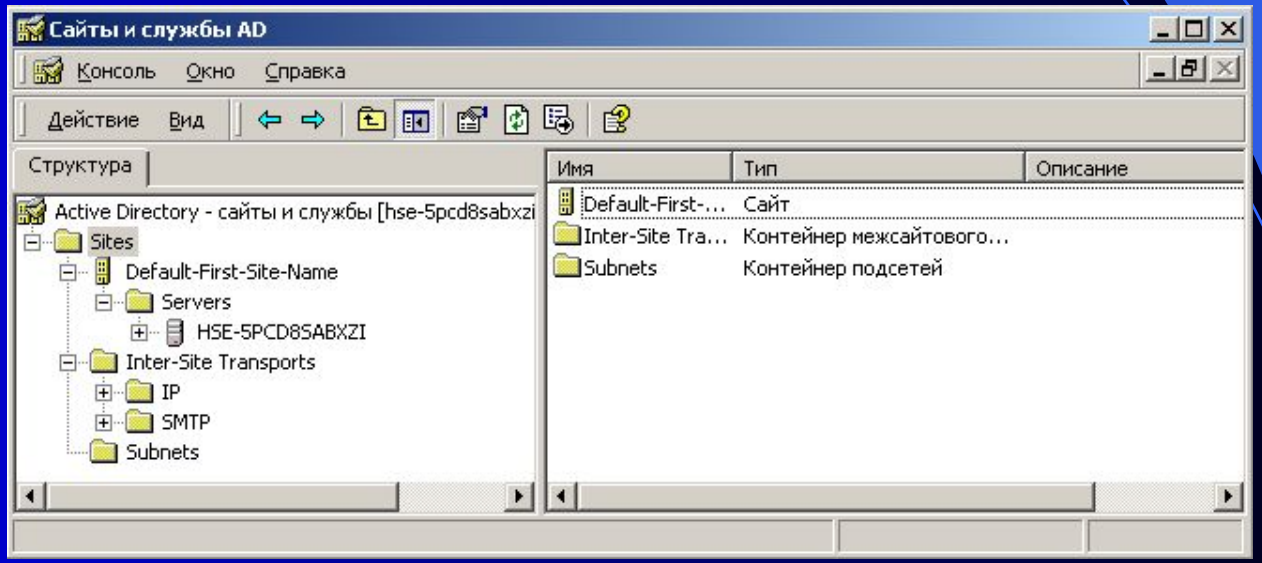
Эмулятор PDC (PDC emulator) – в смешанном режиме домена действует как главный контроллер.

Хозяин инфраструктуры (Infrastructure Master) – обновляет все внутридоменные ссылки на объекты других доменов при изменениях этих объектов.

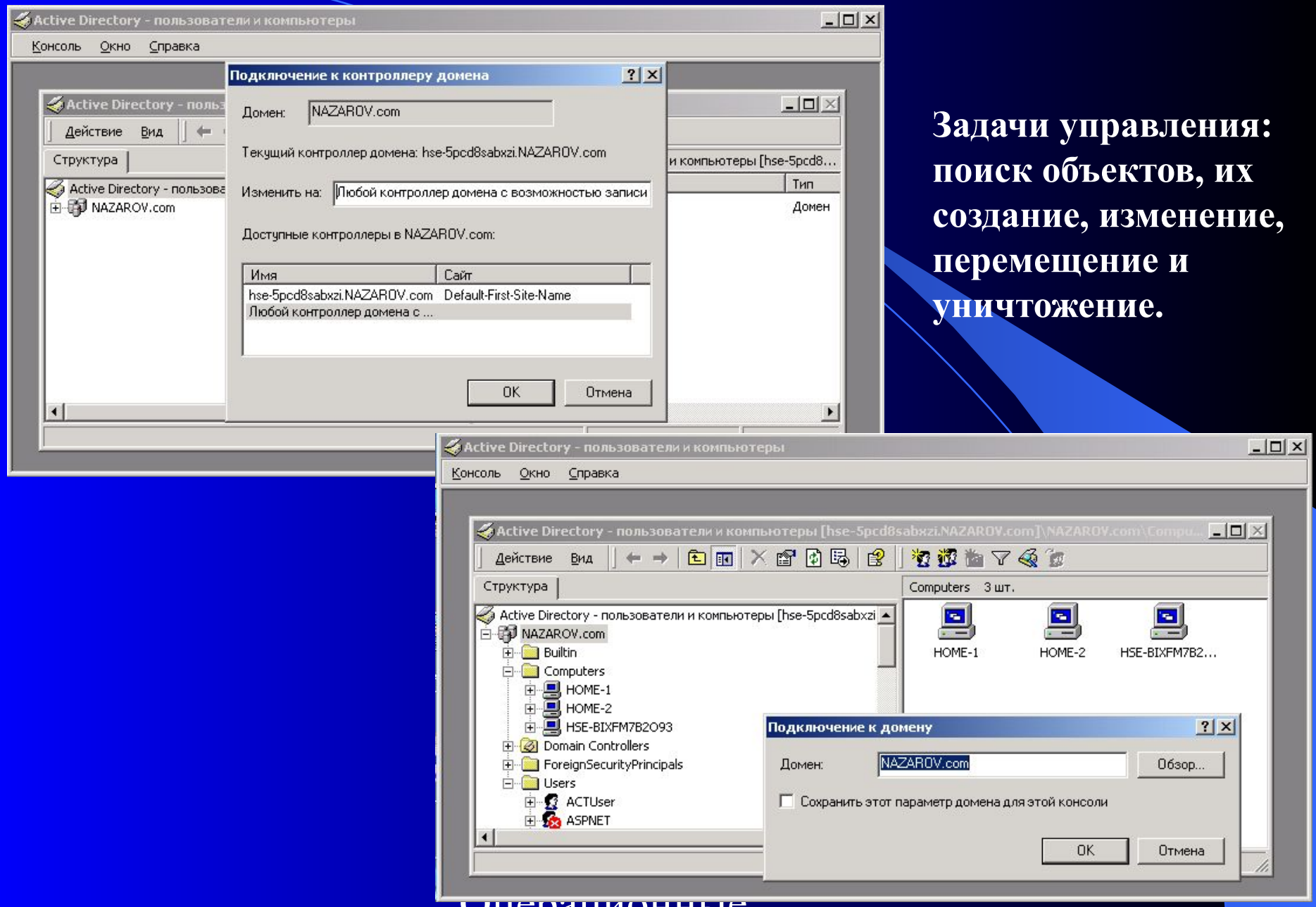
Один домен с несколькими сайтами

Несколько сайтов с несколькими доменами

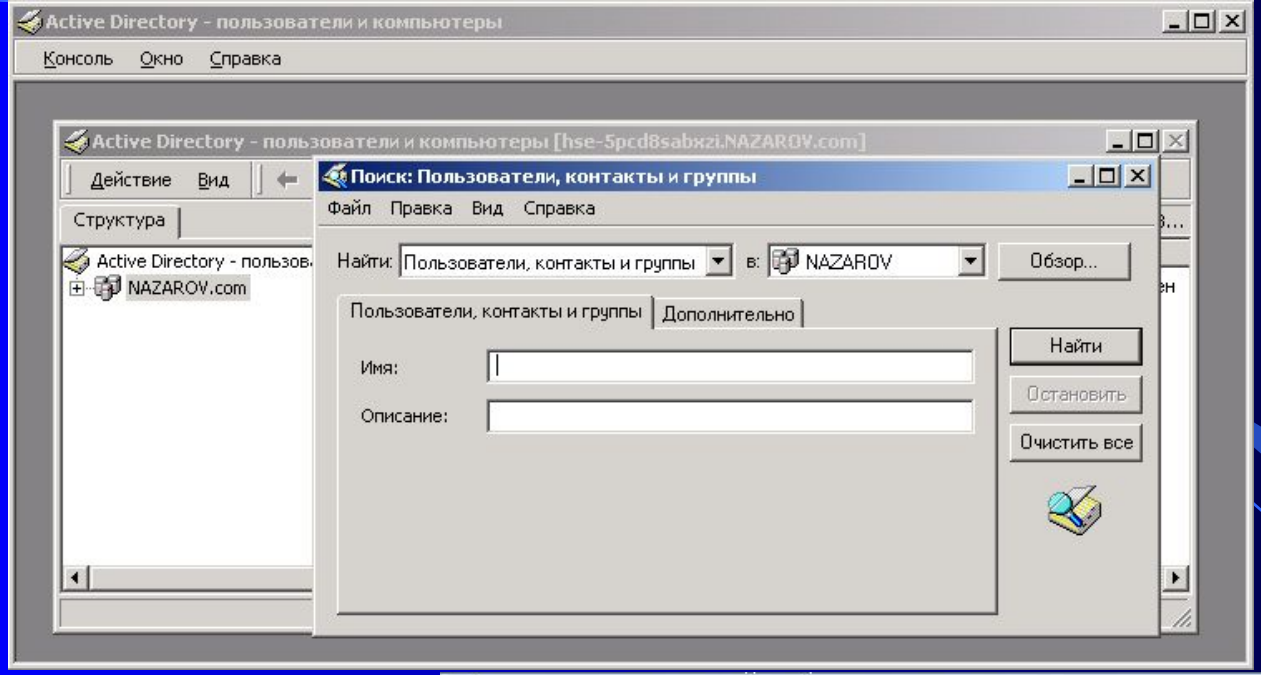


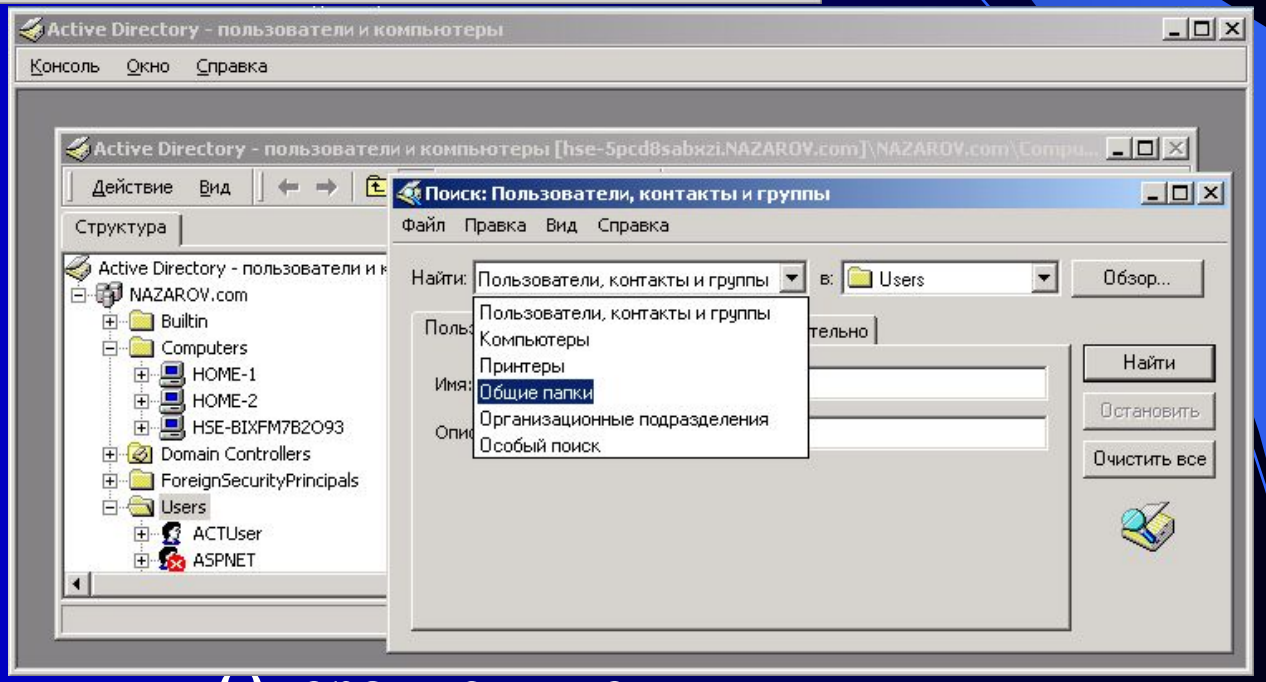


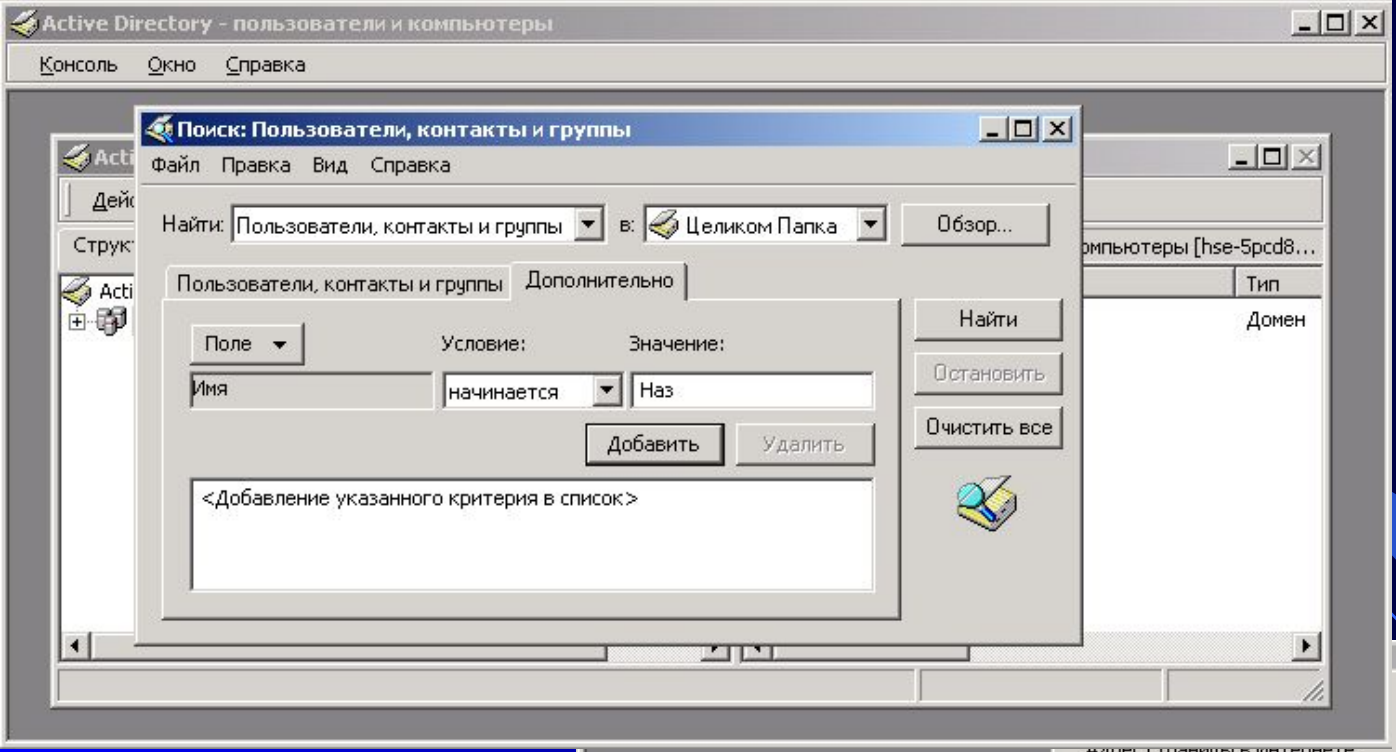
5.7.4. Управление объектами Active Directory

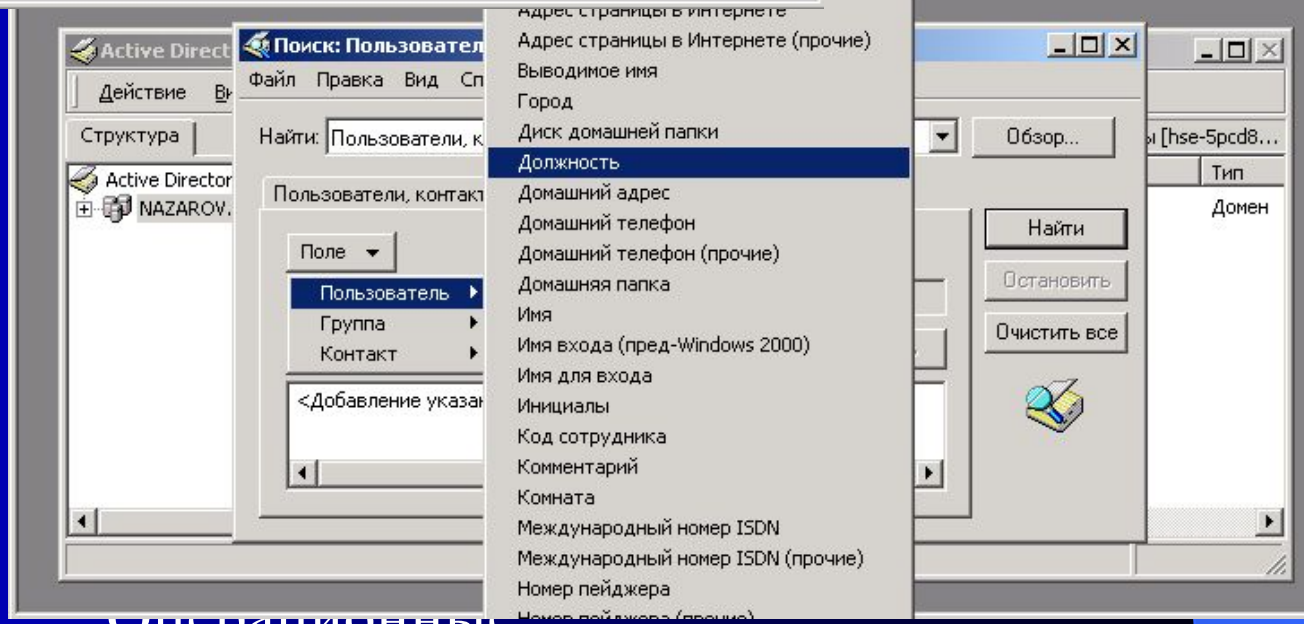


Задачи управления: поиск объектов, их создание, изменение, перемещение и уничтожение.


Active Directory - пользователи и компьютеры
Консоль Окно Справка
Active Directory - пользователи и компьютеры [hse-5pcd8sabxzi.NAZAROV.com]
Действие Вид
Структура
Active Directory - пользов
NAZAROV.com
Поиск: Пользователи, контакты и группы
Файл Правка Вид Справка
Найти: Пользователи, контакты и группы
в: NAZAROV
Обзор...
Пользователи, контакты и группы
Дополнительно
Имя:
Описание:
Найти
Остановить
Очистить все


Active Directory - пользователи и компьютеры
Консоль Окно Справка
Active Directory - пользователи и компьютеры [hse-5pcd8sabxzi.NAZAROV.com]\NAZAROV.com\Compu...
Действие Вид
Структура
Active Directory - пользователи и к
NAZAROV.com
Builtin
Computers
HOME-1
HOME-2
HSE-BIXFM7B2O93
Domain Controllers
ForeignSecurityPrincipals
Users
ACTUser
ASPNET
Поиск: Пользователи, контакты и группы
Файл Правка Вид Справка
Найти: Пользователи, контакты и группы
в: Users
Обзор...
Пользователи, контакты и группы
Компьютеры
Принтеры
Общие папки
Организационные подразделения
Особый поиск
Имя:
Найти
Остановить
Очистить все


Active Directory - пользователи и компьютеры
Консоль Окно Справка
Поиск: Пользователи, контакты и группы
Файл Правка Вид Справка
Найти: Пользователи, контакты и группы в: Целиком Папка Обзор...
Пользователи, контакты и группы Дополнительно
Поле Условие: Значение:
Имя начинается Наз
Добавить Удалить
<Добавление указанного критерия в список>
Найти
Остановить
Очистить все
Тип
Домен

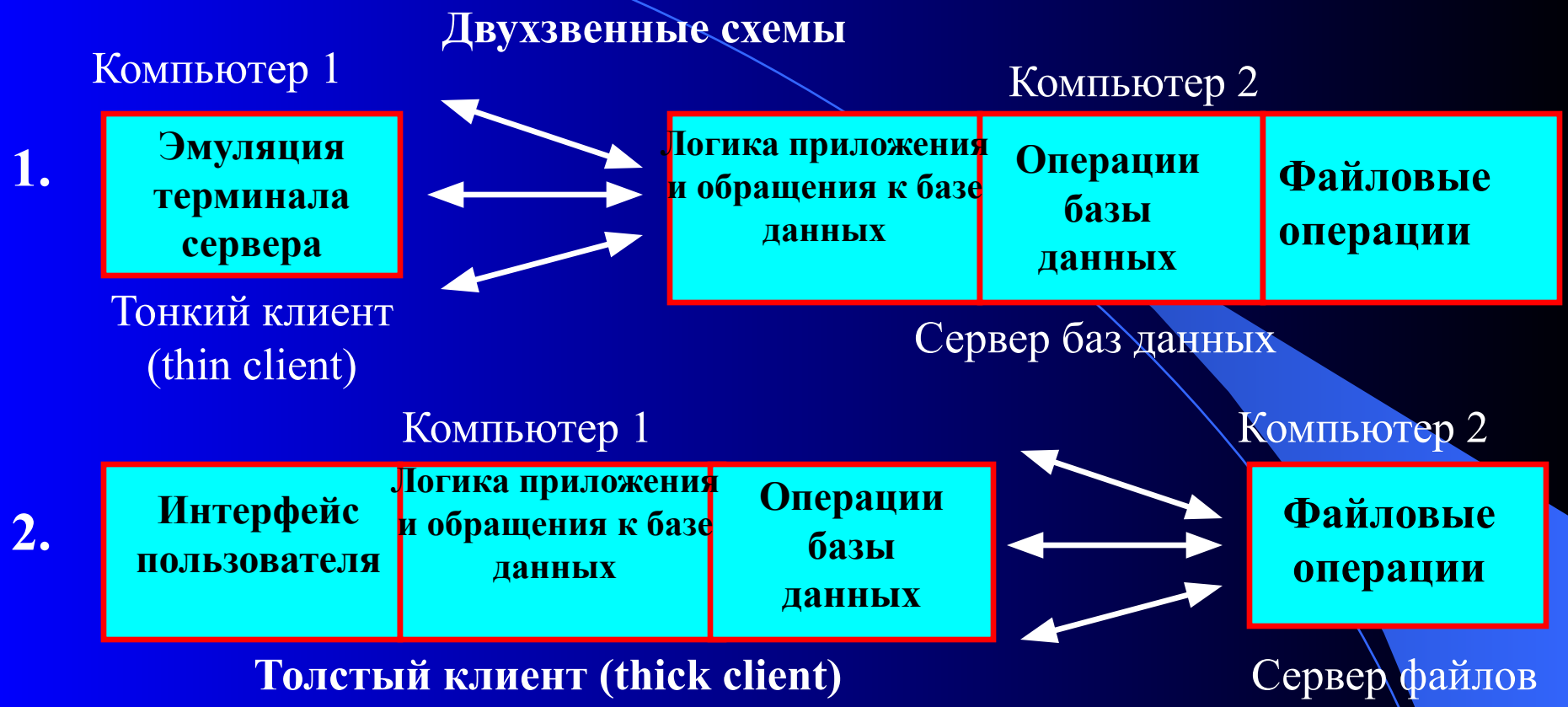

Структура
Пользователь
Группа
Контакт
Адрес страницы в Интернете (прочие)
Выводимое имя
Город
Диск домашней папки
Должность
Домашний адрес
Домашний телефон
Домашний телефон (прочие)
Домашняя папка
Имя
Имя входа (пред-Windows 2000)
Имя для входа
Инициалы
Код сотрудника
Комментарий
Комната
Международный номер ISDN
Международный номер ISDN (прочие)
Номер пейджера
Обзор...
Найти
Остановить
Очистить все
Тип
Домен

5.8. Концепции распределенной обработки в сетевых ОС

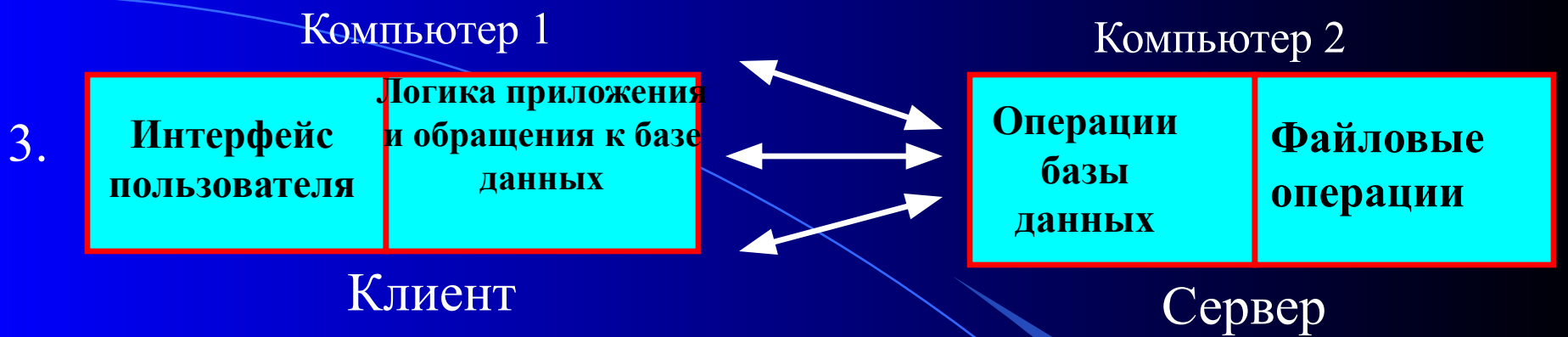
Типовые функциональные части приложений:

1. **Средства представления данных на экране (графический пользовательский интерфейс).**
2. **Логика представления данных на экране – описание правил и возможностей сценариев взаимодействия пользователя с приложением.**
3. **Прикладная логика – набор правил для принятия решения, вычислительные процедуры и операции.**
4. **Логика данных – операции с данными, хранящимися в базе данных, которые нужно выполнить для реализации прикладной логики.**
5. **Внутренние операции базы данных – действия СУБД в ответ на запросы логики данных (поиск записей по определенным признакам).**
6. **Файловые операции – стандартные операции над файлами и файловой системой.**

5.8.1. Модели распределенных приложений



1. Недостаточная масштабируемость и отсутствие отказоустойчивости, ограничение количества клиентов, простота обновления приложений.
2. Хорошая масштабируемость, рост сетевой нагрузки, необходимость обновления приложений на всех клиентских компьютерах.



3. Оптимальное использование сильных сторон сервера и клиента

Трехзвенные схемы

Трехзвенная схема применяется для централизованной реализации в сети общих для распределенных приложений функций, отличных от файлового сервиса и управления базами данных. Программные модули, выполняющие эти функции,относятся к к классу middleware (промежуточному слою). Цель – позволить приложению (клиенту) получить доступ к различным серверным сервисам, не беспокоясь о различиях между серверами.

5.8.2. Передача сообщений в распределенных системах

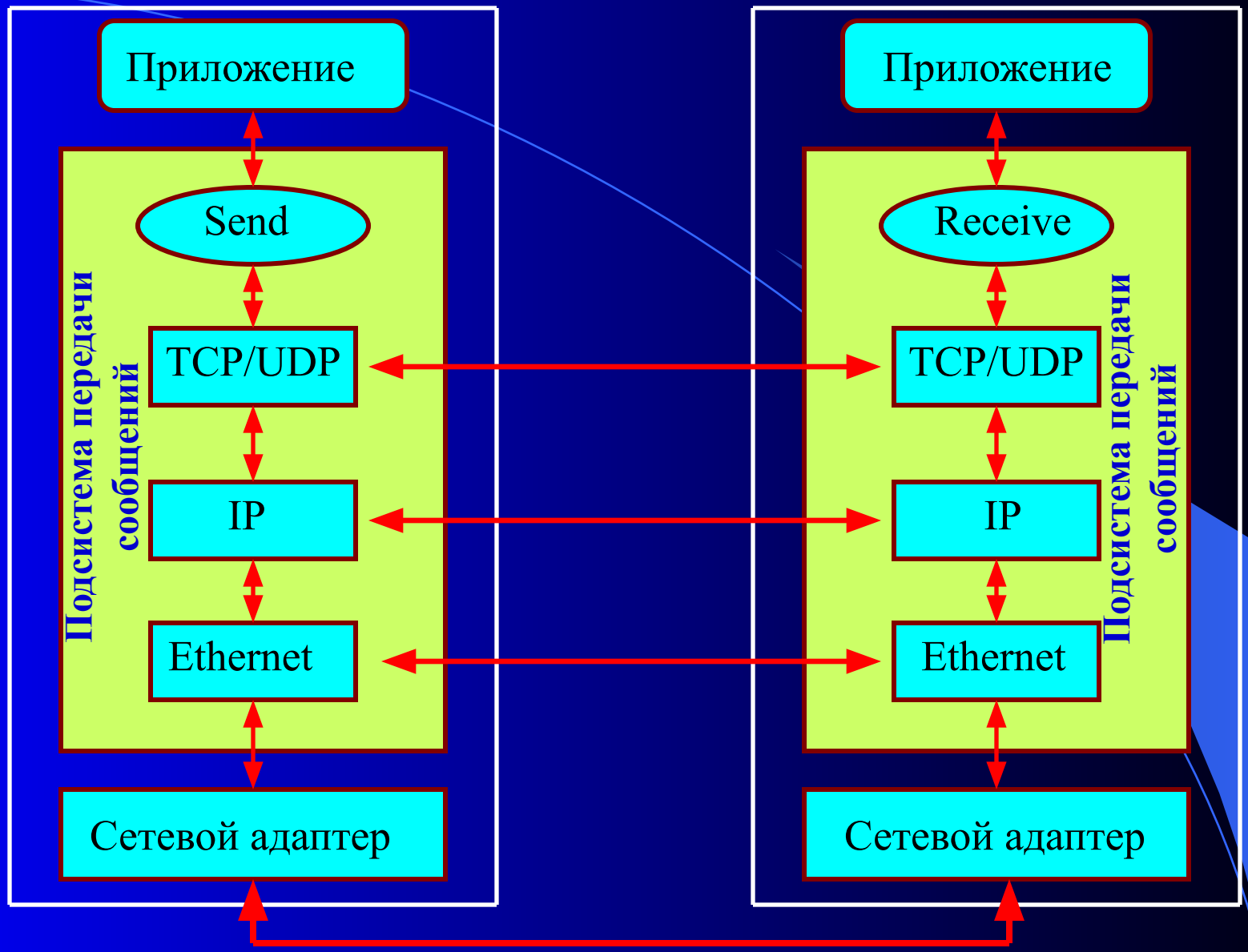
Межпроцессное взаимодействие в компьютерных системах осуществляется:
1) совместным использованием данных, помещенных в разделяемую память;
2) передачей данных в виде сообщений.

Передачей сообщений в распределенных системах управляет транспортная подсистема сетевой операционной системы.

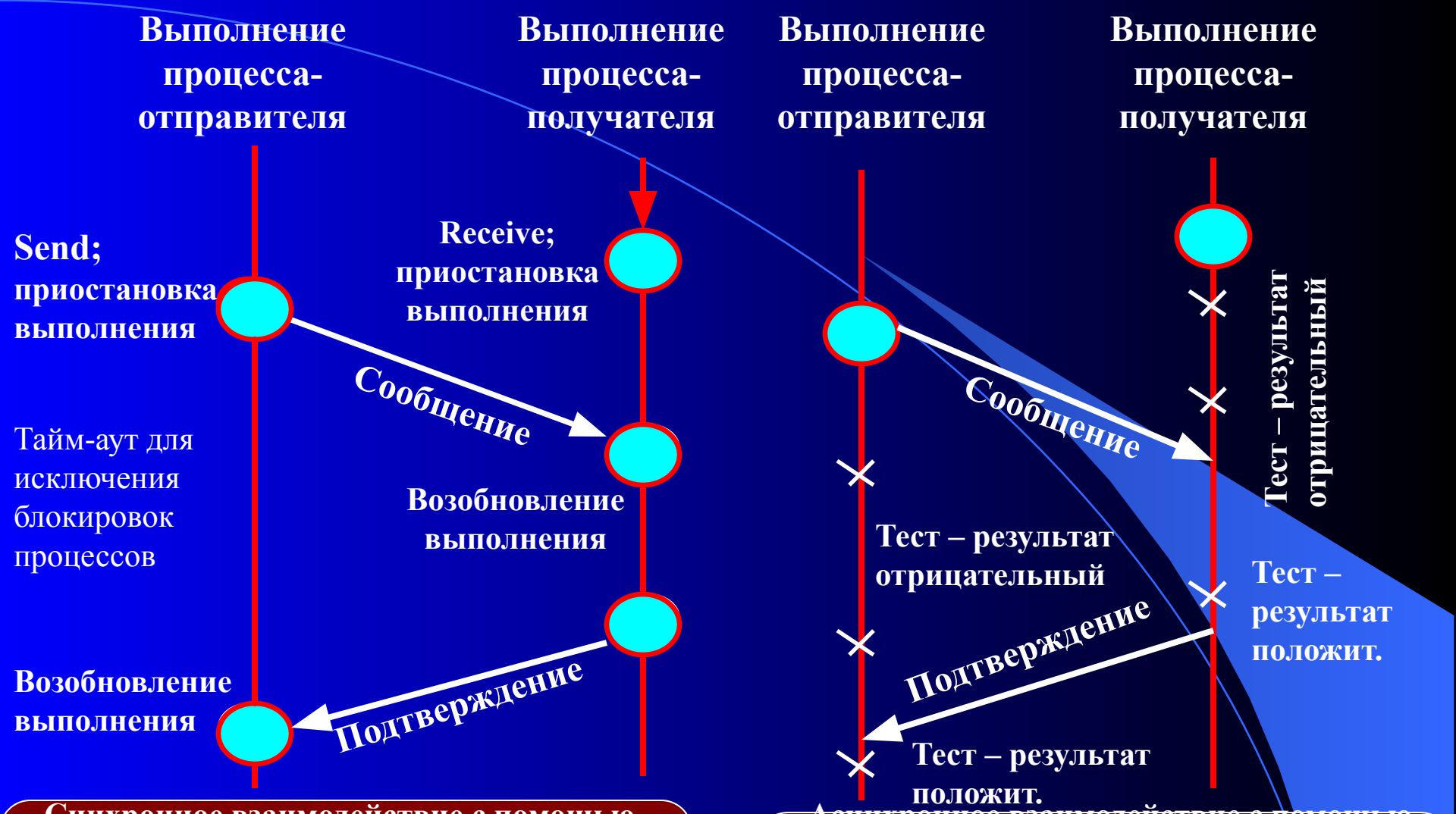
Сообщение – это блок информации, отформатированный процессом-отправителем таким образом, чтобы он был понятен процессу-получателю.

Сообщение состоит из заголовка (обычно фиксированной длины) и набора данных определенного типа переменной длины.

Заголовок содержит: адреса процесса-отправителя и процесса-получателя и идентификатор сообщения (последовательный номер).
Набор данных содержит: 1) поле типа данных, указывающего, какие данные передаются; 2) поле длины данных, определяющее длину передаваемых данных; 3) поле данных, содержащее передаваемые данные.



Способы реализации: внутренние процедуры ядра, системные вызовы, блокирующие или неблокирующие примитивы



Синхронное взаимодействие с помощью блокирующих примитивов Send и Receive.
Достоинства – простота, надежность, необходимость только 1-го буфера. Недостатки – ограниченный параллелизм, возможность клинчей.

Асинхронное взаимодействие с помощью неблокирующих примитивов Send и Receive.
Достоинства – производительность. Недостатки: сложность, необходимость в большом буфере, возможность потерь данных, необходимость в управлении потоком данных.