# Администрирование информационных систем

# Основные задачи администрирования ИС

- Основная цель организации администрирования ИС – реализация на процедурном уровне задачи обеспечения политики информационной безопасности.
- Инструменты администрирования – программные и аппаратные средства, обеспечивающие выполнение политики безопасности.

# Политика безопасности среднего уровня

- К среднему уровню относят вопросы, относящиеся к отдельным аспектам информационной безопасности. Например, организация доступа сотрудников в сеть Интернет или установка и использование ПО.
- Политика среднего уровня для каждого аспекта должна освещать:
  - описание аспекта;
  - область применения;
  - позиция организации по данному вопросу;
  - роли и обязанности;
  - законопослушность;
  - точки контакта.

# Политика безопасности нижнего уровня

- Политика безопасности нижнего уровня относится к работе конкретных информационных сервисов.
- Такая политика включает в себя два аспекта:
  - цели;
  - правила достижения заданных целей.
- Политика безопасности данного уровня быть выражена полно, четко и конкретно. Например, определять сотрудников, имеющих право на работу с конкретной информационной системой и данными.
- Из целей выводятся правила безопасности, описывающие кто, что и при каких условиях может выполнять те или иные процедуры с информационными сервисами.

# Административный уровень защиты информации

- После формулирования политики безопасности, составляется **программа обеспечения информационной безопасности**.
- Программа безопасности также структурируется по уровням. В простом случае достаточно двух уровней:
  - верхнего (центрального) – охватывающего всю организацию;
  - нижнего (служебного) – относящегося к отдельным услугам или группам однородных сервисов.

# Программа верхнего уровня

- Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. Цели такой программы:
  - Управление рисками (оценка рисков, выбор эффективных решений);
  - Координация деятельности в области информационной безопасности
  - Стратегическое планирование
  - Контроль деятельности в области информационной безопасности.
- Контроль деятельности в области ИБ должен гарантировать, во-первых, что действия организации не противоречат законам, во-вторых, что состояние безопасности в организации соответствует требованиям и реагировать на случаи нарушений.

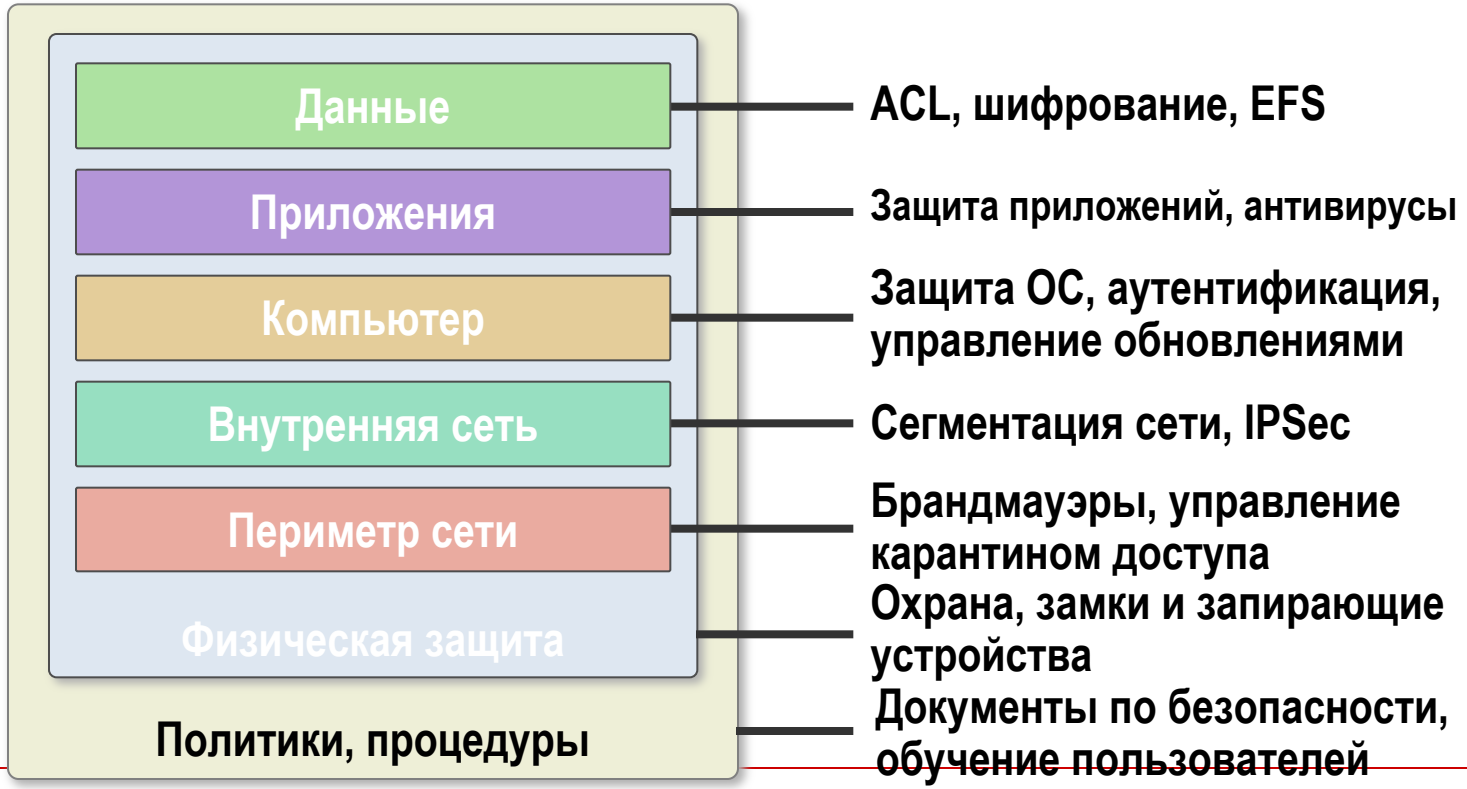
# Программы служебного уровня

- Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов.
- На нижнем уровне осуществляется выбор механизмов защиты, технических и программных средств.
- Ответственность за реализацию программ нижнего уровня обычно несут администраторы соответствующих сервисов.

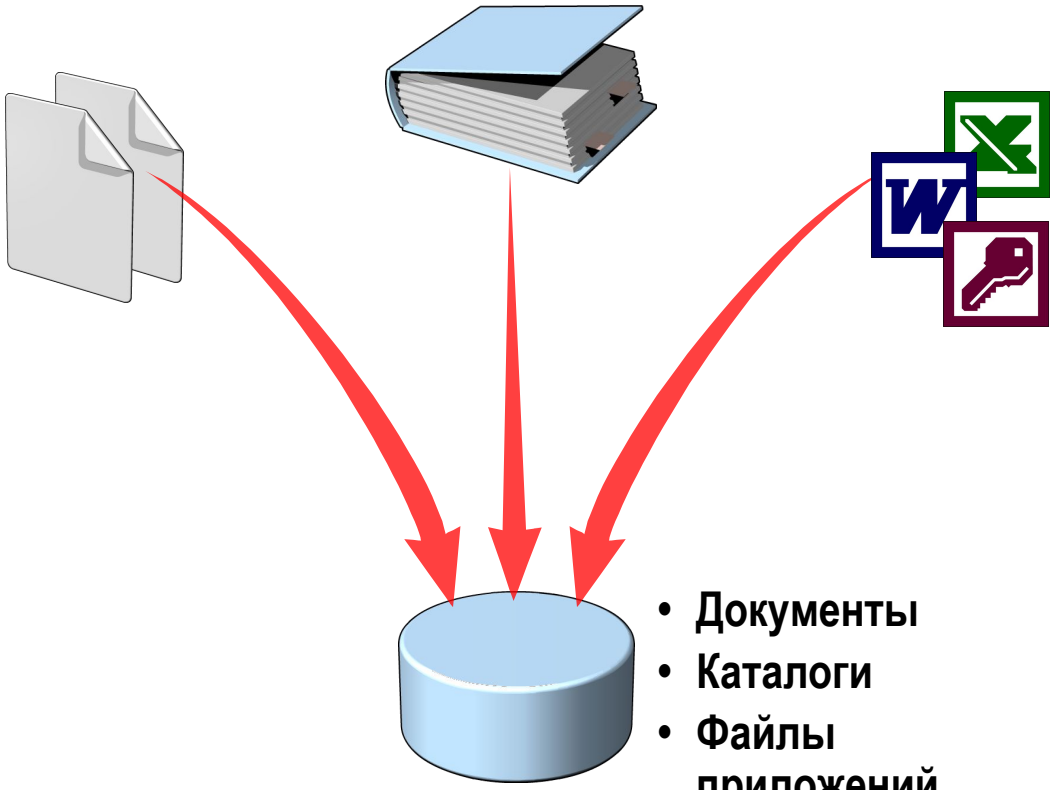
# Модель многослойной защиты

Использование многослойной модели защиты позволяет:

- **Уменьшить шанс успеха атаки**
- **Увеличить вероятность обнаружения атаки**



# Описание уровня данных

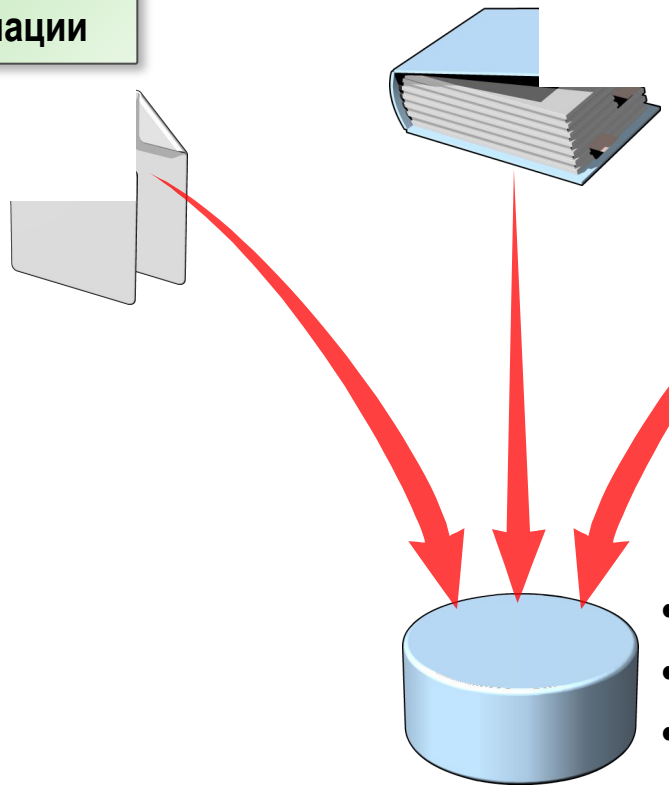


- Документы
- Каталоги
- Файлы приложений

# Угрозы на уровне данных

Просмотр, изменение и удаление информации

Считывание данных каталогов



Подмена и искажение файлов приложений

- Документы
- Каталоги
- Файлы приложений

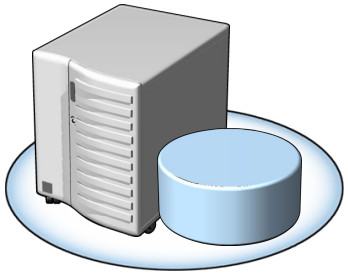
# Задачи администрирования – уровень данных

- На уровне данных задача администрирования – управление доступом к данным.
- Политики управления доступом – дискреционная, мандатная, ролевая.
- Инструменты управления доступом – списки прав доступа (ACL), метки доступа, биты защиты и т.п.
- Доступ к данным регулируется на уровне файловой системы – доступ к файлам, на уровне объектов БД – доступ к таблицам, представлениям.
- Шифрование данных – установка и администрирование PKI.
- Обеспечение регулярного резервного копирования.

# Описание уровня приложений

- Данный уровень включает как клиентскую, так и серверную часть приложения
- Требуется поддержка функционирования

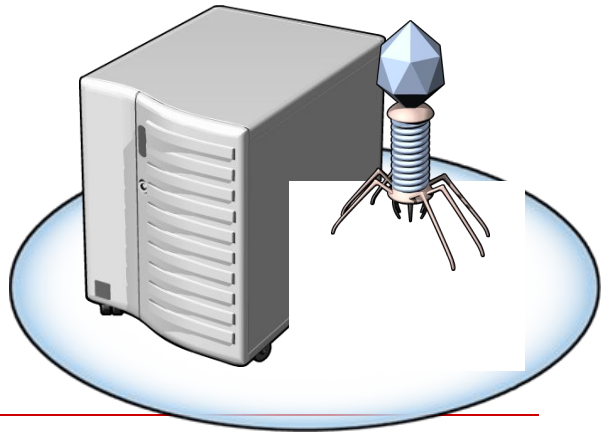
**Клиентские приложения: Microsoft Outlook, Microsoft Office Suite**



**Серверные приложения: Web Servers, Exchange Server, SQL Server**

# Нарушения на уровне приложений

- Потеря функциональности приложения
- Исполнение вредоносного кода
- Чрезмерная нагрузка на приложение – DoS атака
- Нежелательное использование приложения



# Задачи администрирования – уровень приложений

- На уровне приложений основные задачи администрирования – определение прав пользователей на запуск и управление процессами.
- Установление прав доступа к прикладным программам и процессам.
- Управление групповыми политиками на ограничение использования ПК.

# Описание уровня хоста

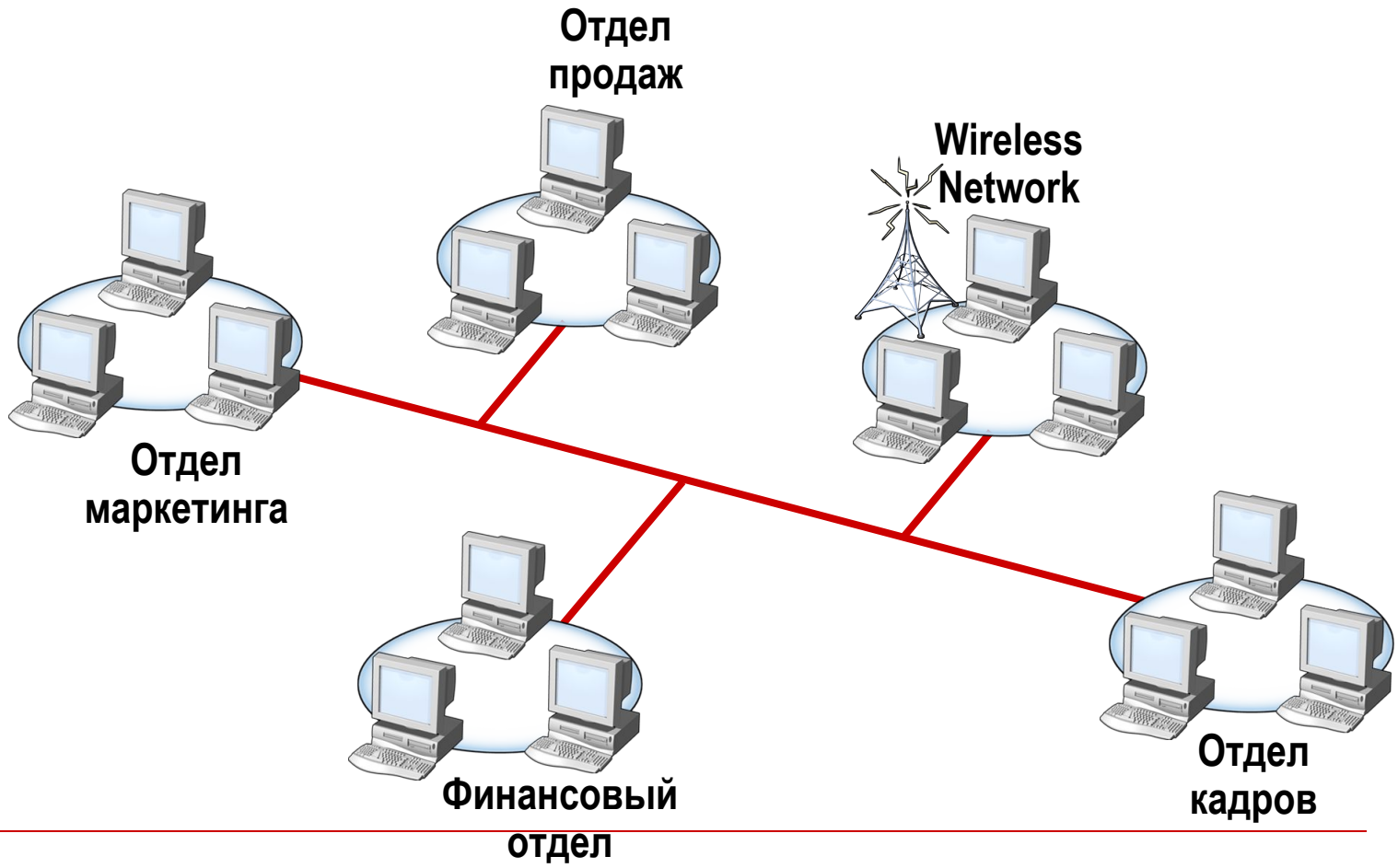
- Включает отдельные ПК пользователей сети
- Часто играет специальную роль в ИС
- Обеспечение ИБ хоста требует баланса между защищенностью и удобством работы пользователя

# Уязвимости уровня хоста

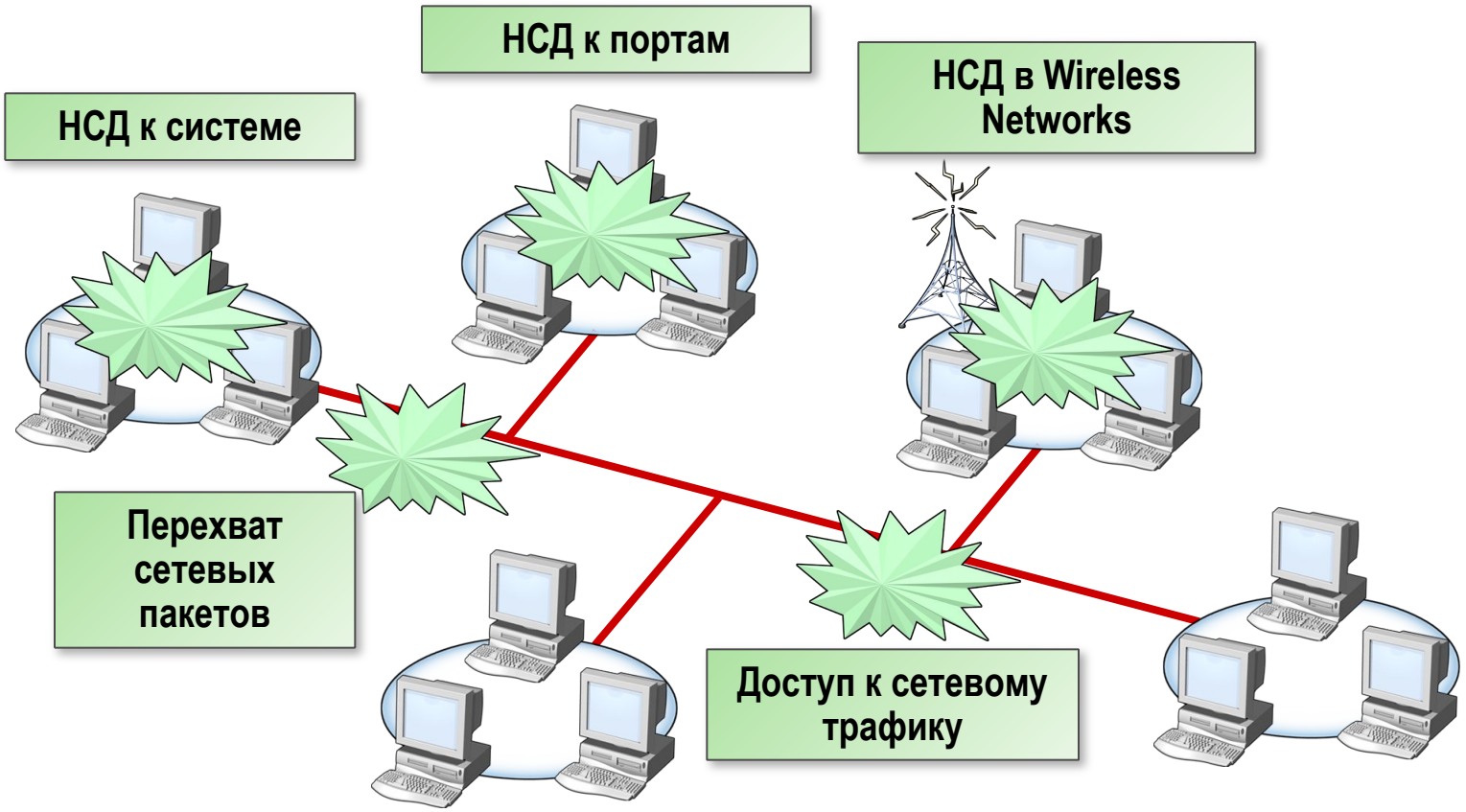
# Задачи администрирования – уровень хоста

- На уровне хоста основные задачи администрирования – определение прав пользователей на работу с компьютером (разграничение входа).
- Определение ограничений на выполнение программ и приложений в вычислительной системе.

# Описание уровня ЛВС



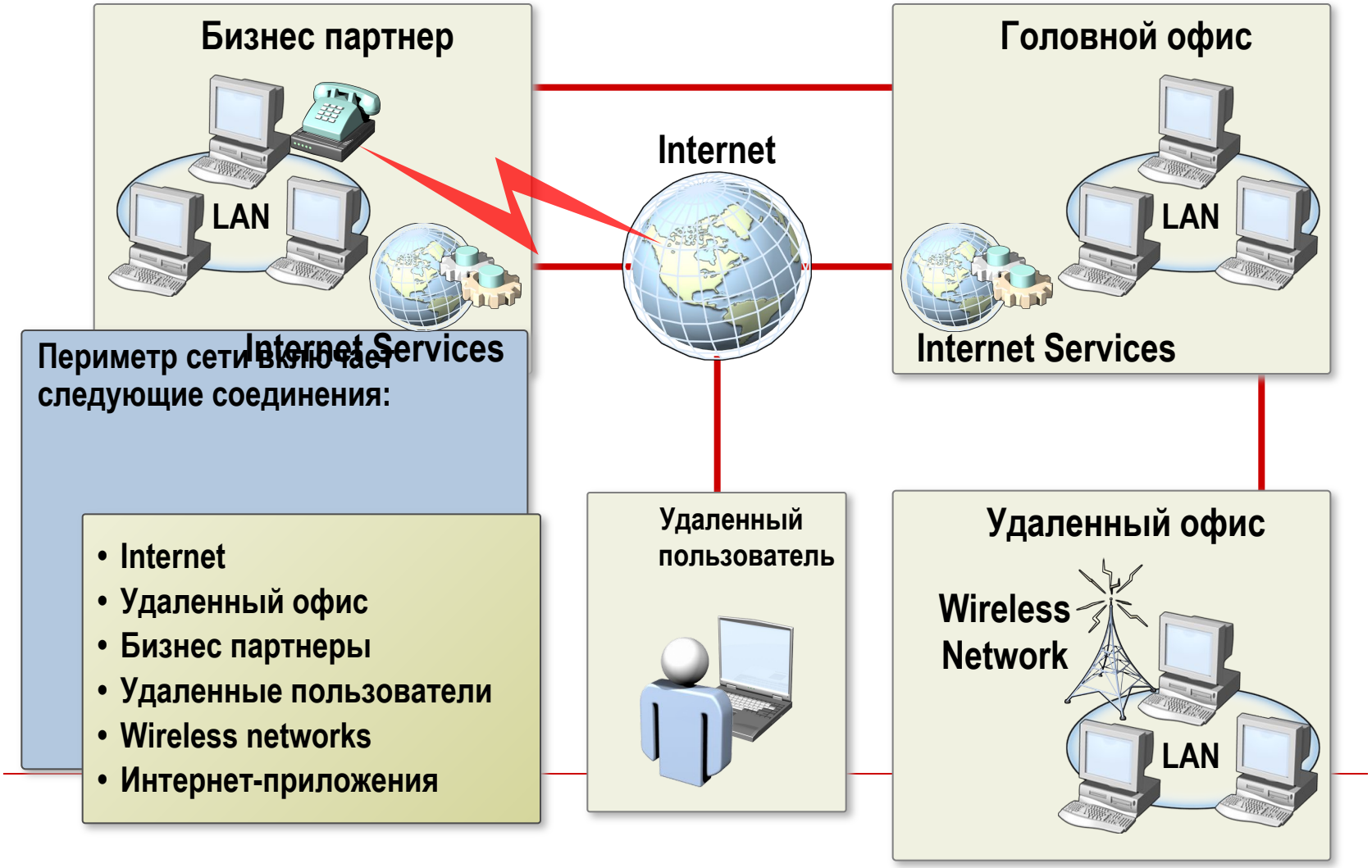
# Нарушения уровня ЛВС



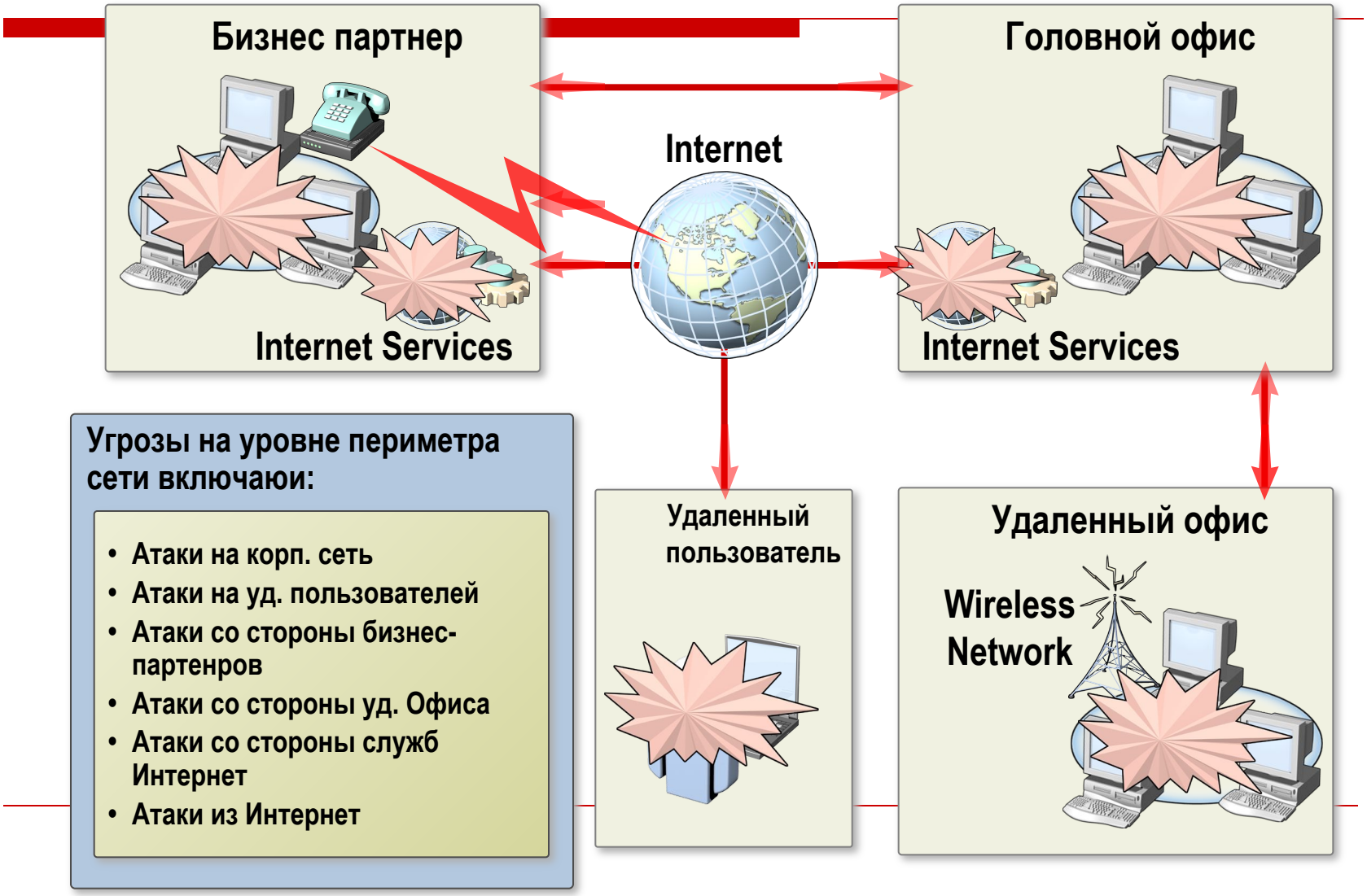
# Задачи администрирования – уровень локальной сети

- На уровне локальной сети основные задачи администрирования – определение прав пользователей на работу в сети (многофакторная аутентификация).
- Использование инфраструктуры открытых ключей – PKI для шифрования трафика.
- Использование служб каталогов для публикации ресурсов и разграничения прав доступа.
- Сегментация сети и администрирование сетевых служб.

# Описание уровня периметра сети



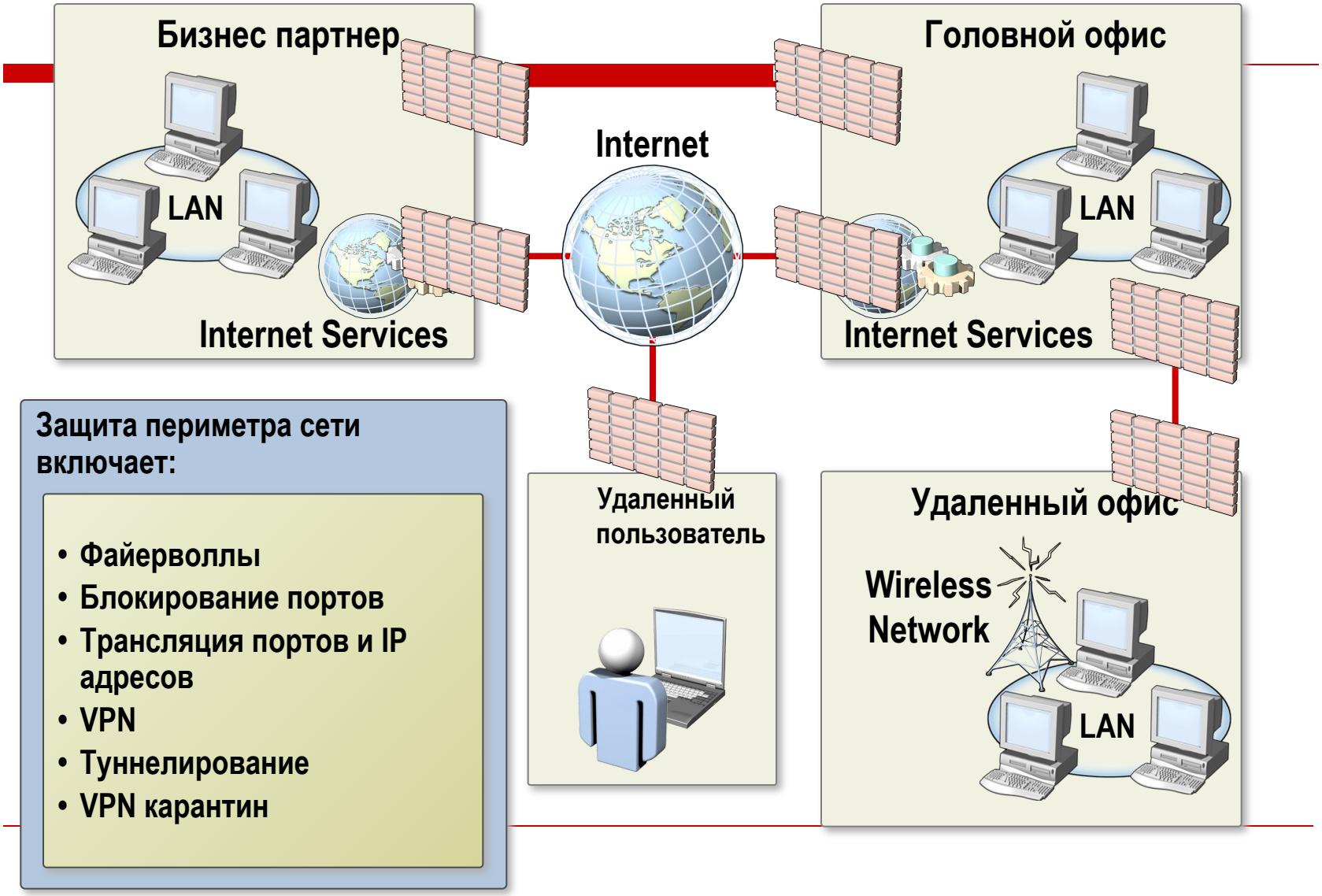
# Угрозы на уровне периметра сети




**Угрозы на уровне периметра сети включаюи:**

- Атаки на корп. сеть
- Атаки на уд. пользователей
- Атаки со стороны бизнес-партенров
- Атаки со стороны уд. Офиса
- Атаки со стороны служб Интернет
- Атаки из Интернет

# Защита на уровне периметра сети




**Защита периметра сети включает:**

- Файерволлы
- Блокирование портов
- Трансляция портов и IP адресов
- VPN
- Туннелирование
- VPN карантин

# Задачи администрирования – уровень периметра сети

- На уровне периметра сети основные задачи администрирования – определение прав пользователей доступ в сеть Интернет из локальной сети и доступ к локальной сети из Интернет.
- Использование инфраструктуры открытых ключей – PKI для шифрования трафика.
- Администрирование инфраструктурных сетевых служб для работы в сети Интернет.
- Администрирование веб-сервисов.

# Компьютерные сети

- Под *вычислительной* (*компьютерной*) *сетью* понимается совокупность компьютеров, объединенных коммуникационной системой и снабженных необходимым программным обеспечением, позволяющим пользователям и приложениям получать доступ к ресурсам удаленных компьютеров.

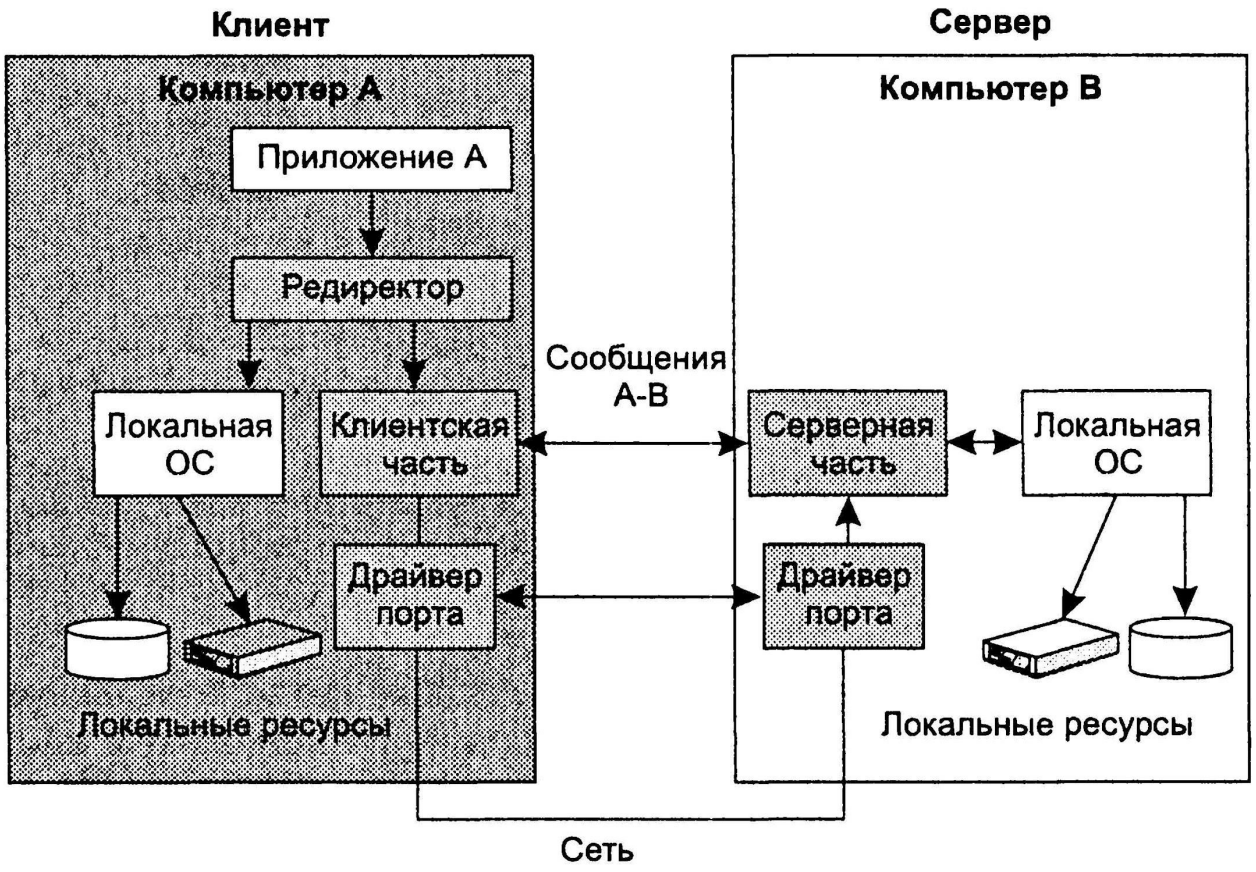
# Сетевые операционные системы

- **Сетевая операционная системы** – комплекс программных модулей, предназначенный для повышения эффективности аппаратных ресурсов компьютера путем рационального управления его ресурсами и разделения ресурсов между множеством выполняемых в сети процессов.
- *Сетевая ОС* обеспечивает пользователю некоторую виртуальную вычислительную систему, упрощающую работу с ней.

# Функциональные компоненты сетевой ОС

- Основные компоненты сетевой ОС:
  - *Средства управления локальными ресурсами* компьютера реализует все функции ОС автономного компьютера (управление процессами, оперативной памятью, управление внешней памятью, пользователями и т.п.)
  - *Сетевые средства,* разделяемые на три компонента:
    - *Серверная часть ОС* – средства предоставления локальных ресурсов и сервисов в общее пользование
    - *Клиентская часть ОС* – средства запроса на доступ к удаленным ресурсам и сервисам
    - *Транспортные средства ОС*, совместно с коммуникационной системой обеспечивающие передачу сообщений между компьютерами

# Взаимодействие двух компьютеров



# Сетевые службы и сервисы

- *Сетевой службой* называется совокупность серверной и клиентской частей ОС, предоставляющих доступ к конкретному типу ресурса компьютера через сеть.
- *Сервис* – интерфейс между потребителем услуг (пользователем или приложением) и поставщиком услуг (службой)

# Типы сетевых ОС

- В зависимости от распределения функций между компьютерами, они могут выступать в роли *выделенного сервера* или *клиентского узла*
- Сеть может быть построена по следующим схемам:
- На основе компьютеров, совмещающих функции клиента и сервера – *одноранговая сеть*
- На основе клиентов и серверов – *сеть с выделенными серверами*
- Сеть, включающая узлы разных типов – *гибридная сеть*.

# Модели сетевых служб и распределенных приложений

- Выделяют три основных параметра организации работы приложений в сети:
  - Способ разделения приложения на части, выполняющиеся на разных компьютерах сети;
  - Выделение специализированных серверов в сети, на которых выполняются некоторые общие для всех приложений функции;
  - Способ взаимодействия между частями приложений, работающих на разных компьютерах.

# Способы разделения приложений на части

- Приложения условно можно разделить на следующие функциональные части:
  - Средства представления данных на экране;
  - Логика представления данных на экране (описывает правила и сценарии взаимодействия пользователя с приложениями);
  - Прикладная логика (правила для принятия решений, вычислительные процедуры и т.п.);
  - Логика данных – операции с данными, хранящимися в некоторой базе;
  - Внутренние операции БД – действия СУБД, вызываемые в ответ на выполнение запросов логики данных;
  - Файловые операции – стандартные операции над файлами и файловой системой.

# Двухзвенные схемы

- Двухзвенные схемы описывают разделение функций приложения между двумя компьютерами:
  - Централизованная обработка данных;
  - Схема «файл-сервер»
  - Схема «клиент-сервер»

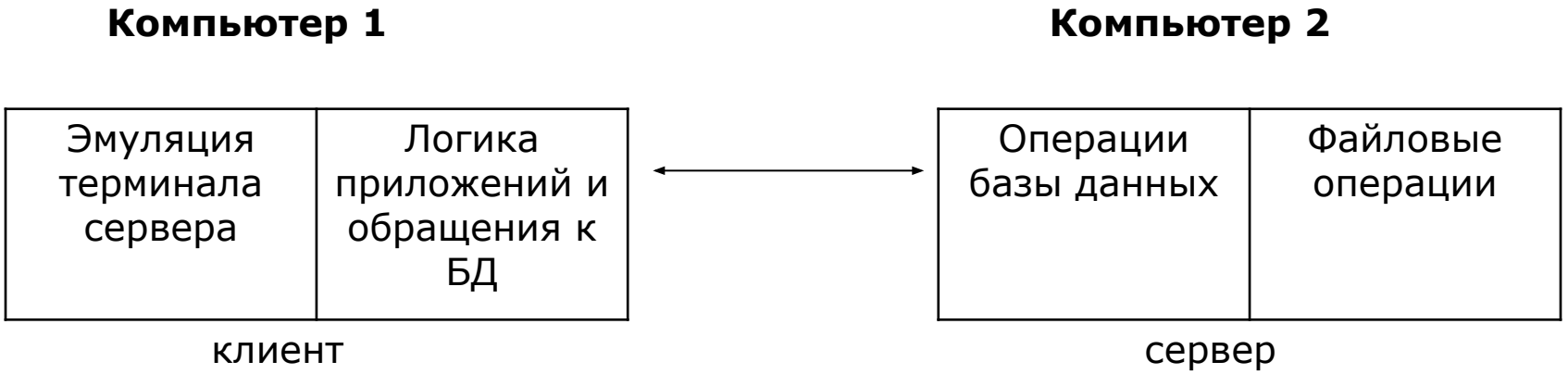
# Централизованная обработка данных


- Достоинства схемы:
  - Ресурсы клиентского компьютера используются в незначительной степени, загружаются только графические средства ввода-вывода;
  - Простота организации программы;
- Недостатки схемы:
  - Недостаточная масштабируемость;
  - Отсутствие отказоустойчивости.

# Схема «файл-сервер»

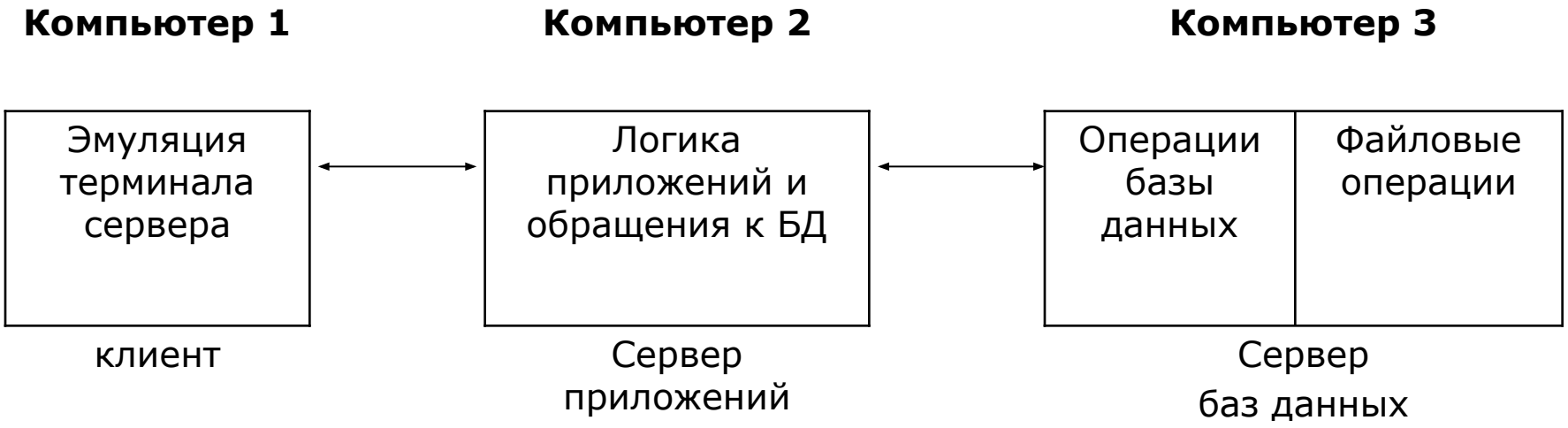

- Достоинства схемы:
  - Данная схема обладает хорошей масштабируемостью, поскольку дополнительные пользователи и приложения добавляют лишь незначительную нагрузку на центральный узел – файловый сервер.
- Недостатки схемы:
  - Во многих случаях возрастает нагрузка, что приводит к увеличению времени реакции на приложения;
  - Клиентский компьютер должен обладать высокой вычислительной мощностью, чтобы справляться с представлением данных, логикой приложений, логикой данных и поддержкой операции БД

# Схема «клиент-сервер»




- Достоинства схемы:
  - Данная схема более равномерно распределяет функции между клиентской и серверной частями системы;
- Клиентский компьютер выполняет функции, специфические для данного приложения;
- Сервер – функции, реализация которых не зависит от специфики приложения, и данные функции могут быть оформлены в виде сетевых служб.

# Многозвенные схемы

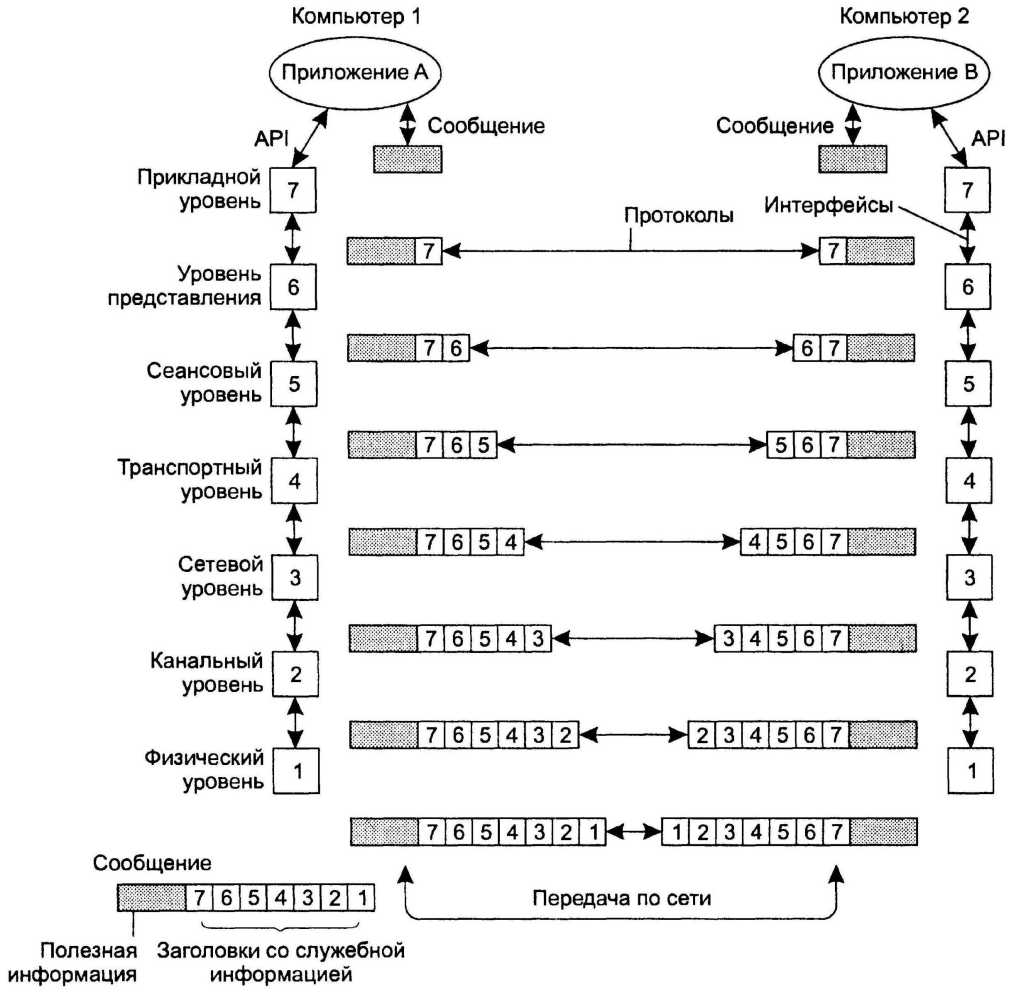



- Централизованная реализация логики приложения решает проблему недостаточной вычислительной мощности клиентских компьютеров для сложных приложений, упрощает администрирование и поддержку системы;
- Упрощается разработка крупных приложений, поскольку четко разделены платформы и инструменты для реализации интерфейса и прикладной логики.

# Основы межсетевого обмена

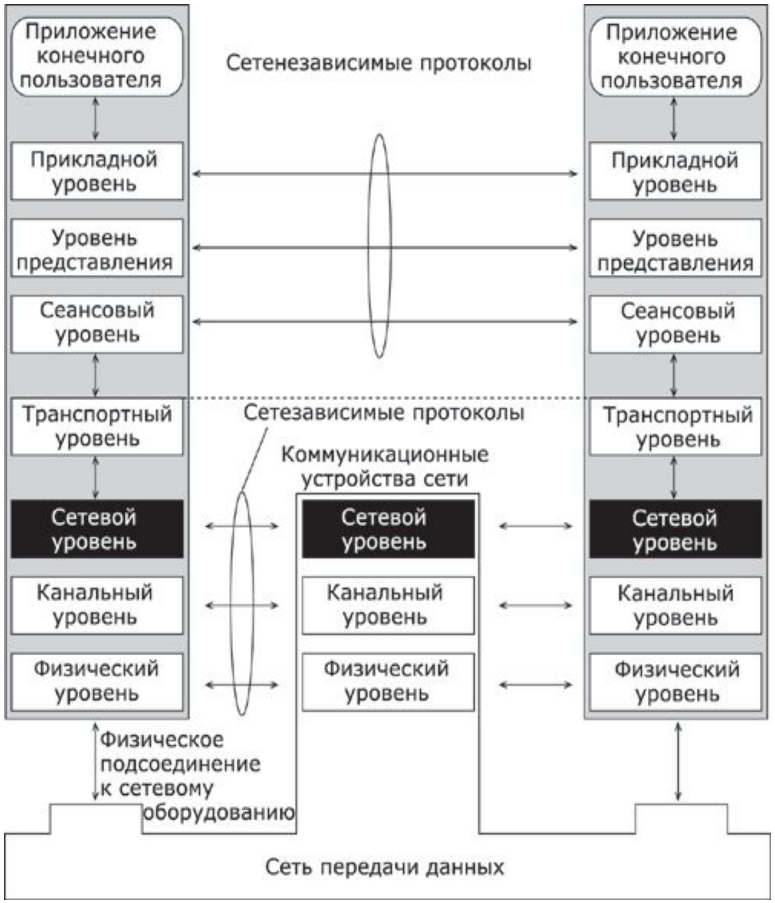
- При рассмотрении процедур межсетевого взаимодействия всегда опираются на стандарты, разработанные *International Standard Organization (ISO)*.
- Данные стандарты называются "Семиуровневой модели сетевого обмена" или в английском варианте *"Open System Interconnection Reference Model" (OSI Ref.Model)*.
- В модели OSI обмен информацией может быть представлен в виде стека, представленного на рисунке.
- В рамках данной модели определяется все аспекты соединения – от стандарта физического соединения сетей до протоколов обмена прикладного программного обеспечения.

# Эталонная модель взаимодействия откртытых систем



# Модель OSI

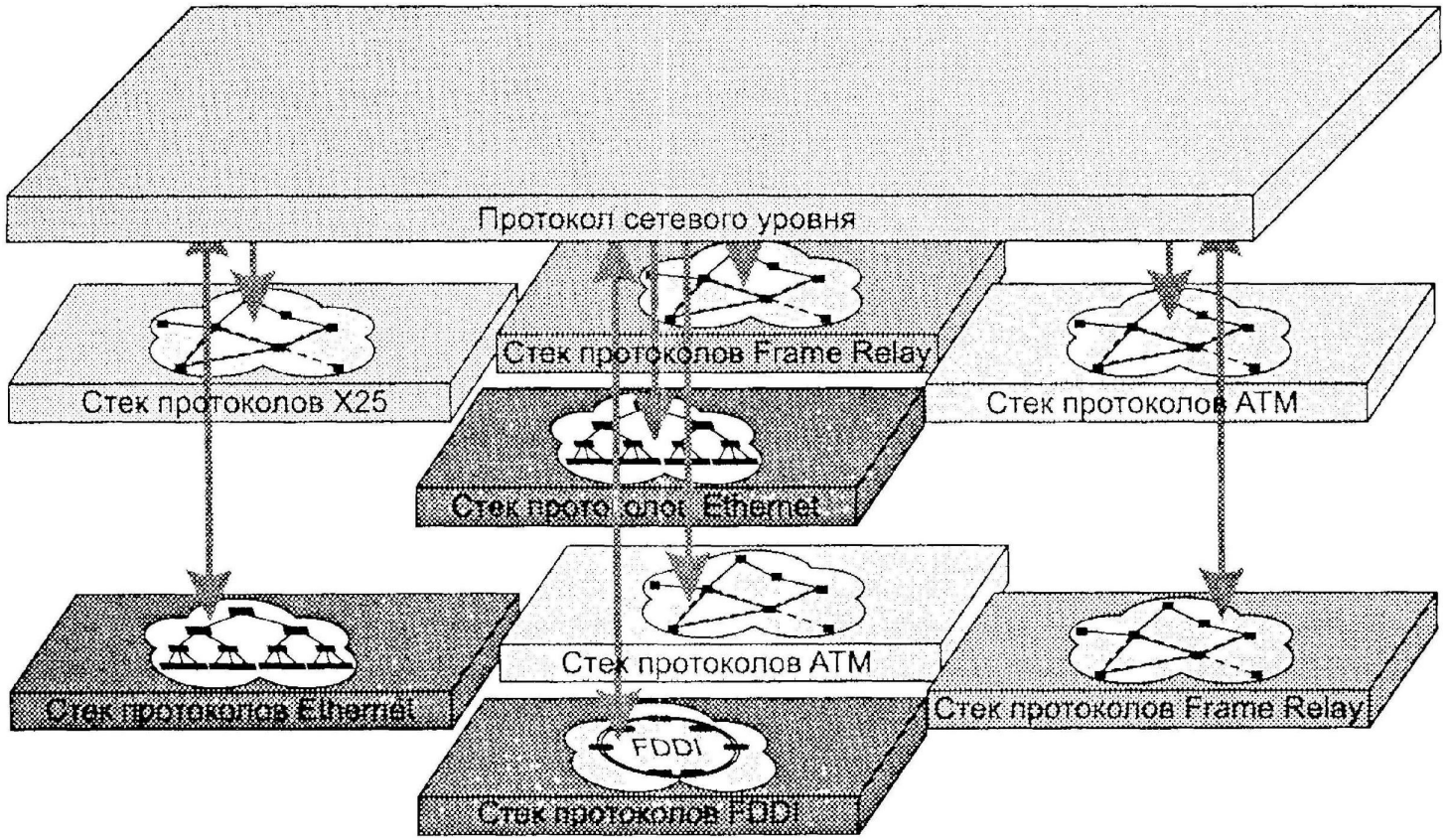
- Нижние уровни (с 1 по 3) модели OSI управляют физической доставкой сообщений и их называют *уровнями среды передачи данных (media layers)*.
- Верхние уровни (с 4 по 7) модели OSI призваны обеспечить точную доставку данных между компьютерами в сети и их называют *уровнями хост-машины (host layers)*.
- Модель OSI *не является* схемой реализации сети, она только определяет функции каждого уровня.



# Уровни в модели OSI

- *Физический уровень* модели определяет характеристики физической сети передачи данных, которая используется для межсетевого обмена. Это такие параметры, как: напряжение в сети, сила тока, число контактов на разъемах и т.п. Типичными стандартами этого уровня являются, например RS232C, V35, IEEE 802.3 и т.п.
- *Канальный уровень* включает протоколы, определяющие соединение, например, SLIP (Strial Line Internet Protocol), PPP (Point to Point Protocol), NDIS, пакетный протокол, ODI и т.п. Речь идет о протоколе взаимодействия между драйверами устройств и устройствами, с одной стороны, а с другой стороны, между операционной системой и драйверами устройства. Драйвер – представляет собой конвертор данных из оного формата в другой, но при этом он может иметь и свой внутренний формат данных.
- К *сетевому (межсетевому) уровню* относятся протоколы, которые отвечают за отправку и получение данных, или, другими словами, за соединение отправителя и получателя. К данному уровню в TCP/IP относят протокол IP (Internet Protocol). На данном уровне определяется отправитель и получатель, именно здесь находится необходимая информация для доставки пакета по сети.

# Взаимодействие на сетевом уровне



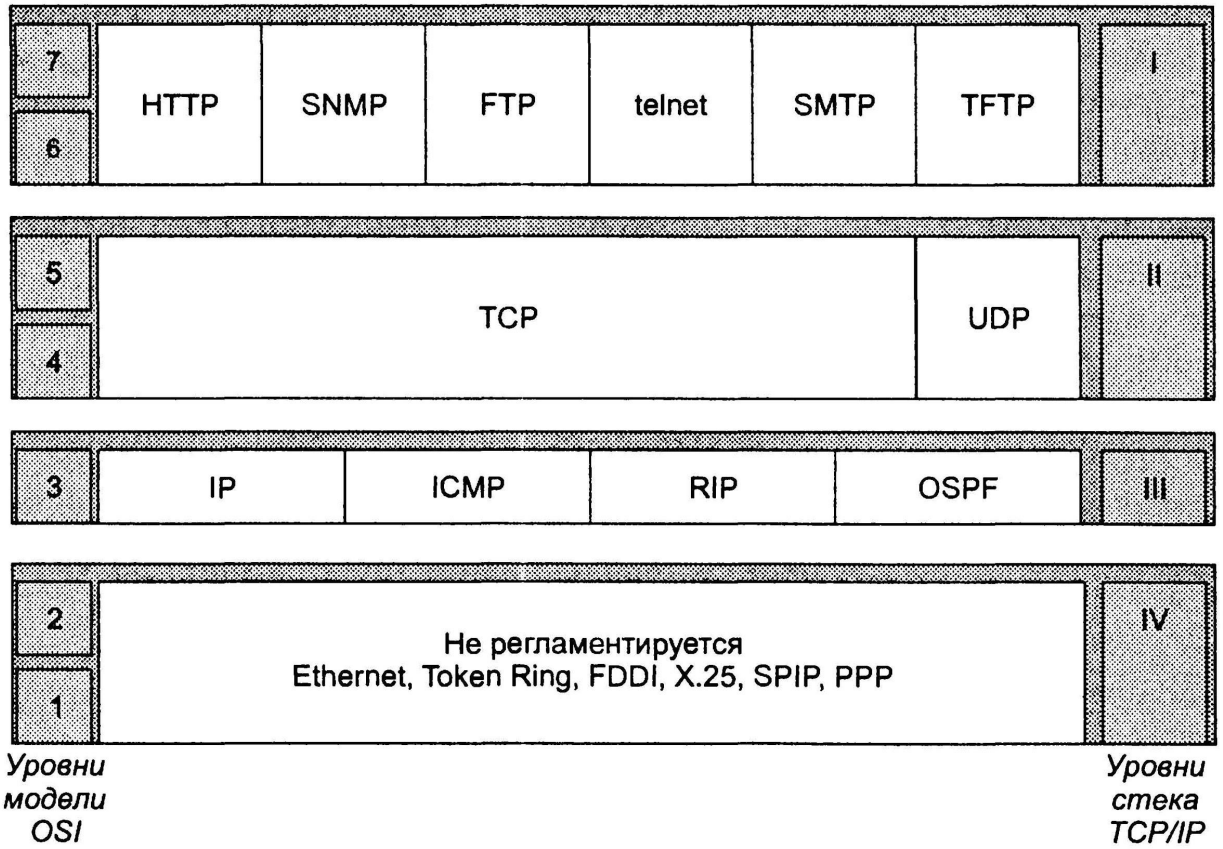
# Уровни в модели OSI

- *Транспортный уровень* отвечает за надежность доставки данных, и здесь, проверяя контрольные суммы, принимается решение о сборке сообщения в одно целое.
- *Уровень сессии* определяет стандарты взаимодействия между собой прикладного программного обеспечения. Это может быть некоторый промежуточный стандарт данных или правила обработки информации. Условно к этому уровню можно отнеси механизм портов протоколов TCP и UDP и Berkeley Sockets.
- *Уровень обмена данными с прикладными программами* (Presentation Layer) необходим для преобразования данных из промежуточного формата сессии в формат данных приложения.
- *Уровень прикладных программ или приложений* определяет протоколы обмена данными этих прикладных программ.

# Стек TCP/IP

- Стек TCP/IP был разработан по инициативе Министерства обороны США (DoD) более 20 лет назад для связи экспериментальной сети ARPANET с другими сетями как набор общих протоколов для разнородной вычислительной среды.
- Большой вклад в развитие стека TCP/IP, который получил свое название по популярным протоколам IP и TCP, внес университет Беркли, реализовав протоколы стека в своей версии ОС Unix.
- Популярность этой операционной системы привела к широкому распространению протоколов TCP, IP и других протоколов стека.

# Архитектура стека TCP/IP



# Особенности протоколов TCP/IP

- Свойством, делающим возможным применение этого протокола в больших сетях, является его *способность фрагментировать пакеты.*
- Большая составная сеть часто состоит из сетей, построенных на совершенно разных принципах. В каждой из этих сетей может быть собственная величина максимальной длины единицы передаваемых данных (кадра).
- При переходе из одной сети, имеющей большую максимальную длину, в сеть с меньшей максимальной длиной может возникнуть необходимость деления передаваемого кадра на несколько частей. Протокол IP стека TCP/IP эффективно решает эту задачу.

# Особенности протоколов TCP/IP

- Другой особенностью технологии TCP/IP является *гибкая система адресации,* позволяющая проще, чем другие протоколы аналогичного назначения включать в составную сеть сети разных технологий. Это свойство также способствует применению стека TCP/IP для построения больших гетерогенных сетей.
- В стеке TCP/IP очень *экономно используются широковещательные рассылки.* Это свойство совершенно необходимо при работе на медленных каналах связи, характерных для территориальных сетей.

# Глобальные сети

- *Глобальные сети (WAN)*, называемые также территориальные компьютерные сети, обеспечивают различные сервисы большому количеству конечных абонентов, разнесенных по значительной территории.
- В силу значительных размахов построение глобальной сети требует очень больших затрат на создание и поддержку работоспособности сети.

# Провайдеры услуг

- Глобальные сети создаются крупными телекоммуникационными компаниями для оказания услуг абонентам.
- **Оператор сети** – компания обеспечивающая поддержку работоспособности сети;
- **Провайдер услуг** – компания, оказывающая услуги (как правило, платные) абонентам сети.
- Владелец, оператор и поставщик услуг могут представлять одну компанию или различные организации.

# Сети операторов связи

- Сети, которые создаются специально для оказания *общедоступных (публичных, public) телекоммуникационных услуг*. Примерами таких сетей могут служить городские, региональные, национальные и международные *телефонные сети*.
- Их услугами пользуются многочисленные **клиенты** - владельцы домашних и мобильных телефонов, а также предприятия (корпоративные пользователи). Еще одной традиционной телекоммуникационной услугой является предоставление в аренду *каналов связи*.
- У *первичных сетей* PDH/SDH, создаваемых телекоммуникационным предприятием для объединения своих АТС, обычно остается не используемая для внутренних нужд канальная емкость, которую логично сдавать в аренду. Типичными потребителями этой услуги являются крупные предприятия, которые создают с помощью арендованных *каналов* собственные сети - *телефонные* или *компьютерные*.

# Частные сети

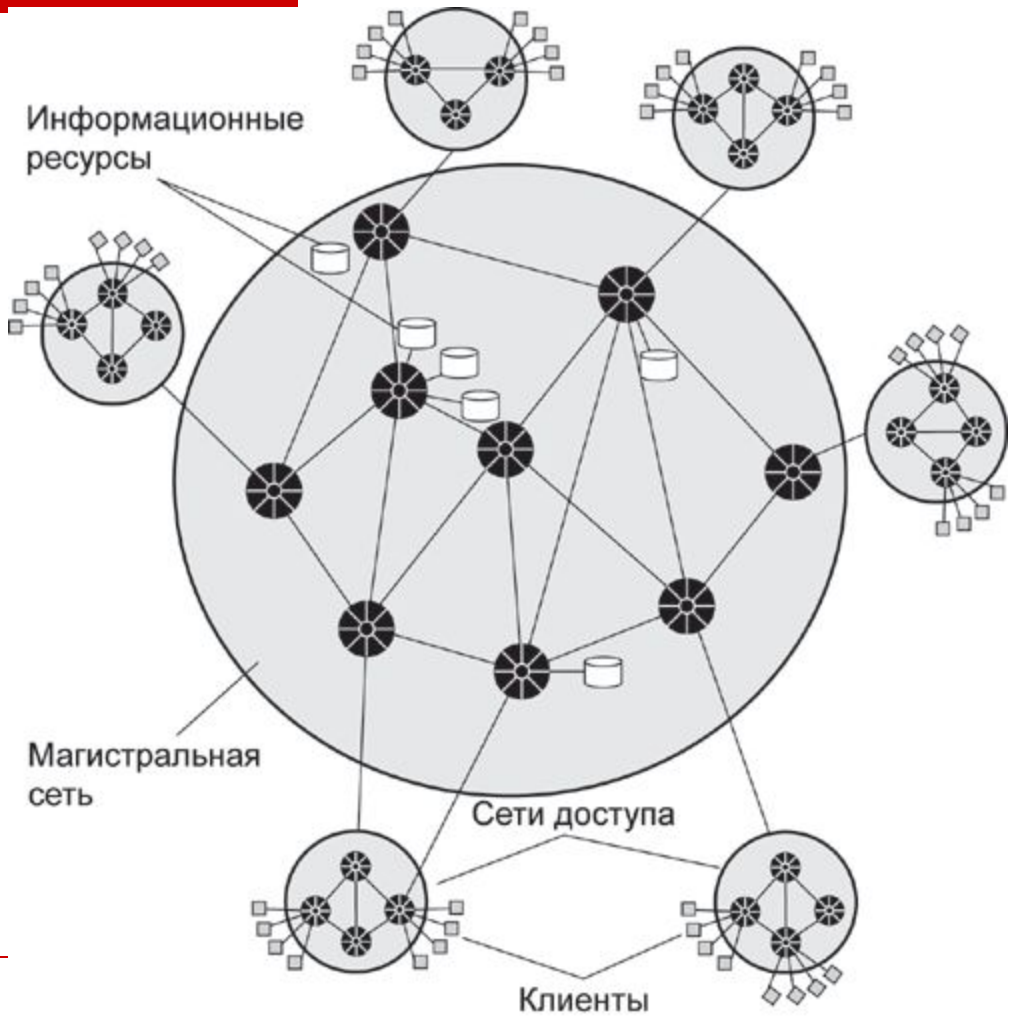
- К набору телекоммуникационных услуг добавилась возможность объединения локальных сетей предприятий с помощью общедоступной территориальной сети передачи данных, например сети технологии X.25, frame relay, ATM или IP.
- На стыке *телефонных* и *компьютерных сетей* начали появляться новые типы общедоступных услуг, использующие возможности комплексного применения различных технологий.
- Глобальные сети, создаваемые крупными корпорациями для собственных нужд и доступные исключительно для пользователей данной организации называются *частными*.
- Для организации объединенной сети корпорации чаще используется промежуточный вариант – корпоративная сеть пользуется услугами публичной, добавляя собственные оборудование и сервисы. Например, аренда каналов передачи данных у операторов связи.

# Высокоуровневые услуги глобальных сетей

- Транспортные функции глобальных сетей обеспечивают услуги трех нижних уровней модели OSI – физического, канального и сетевого.
- Функции глобальных сетей, относящихся к верхним уровням протокола, в последнее время играют заметную роль в вычислительных сетях.
- Основную роль играет развитие публичной сети Интернет. Список высокоуровневых услуг сети Интернет достаточно широк:
  - Доступ к гипертекстовой информации;
  - Широковещательное распространение звукозаписи и видеозаписи;
  - Видеоконференцсвязь;
  - Организация интерактивных бесед;
  - Поиск информации и ее доставка и т.д.

# Общая структура глобальной сети

- *Телекоммуникационная сеть* в общем случае включает следующие компоненты:
  - ***сеть доступа (access network);***
  - ***магистраль (backbone или core network)***;
  - ***информационные центры*** или центры управления сервисами **(data centers или services control point)**.



# Структура глобальной сети

- Компоненты глобальной сети:
  - ***сеть доступа (access network)*** - предназначена для концентрации информационных потоков, поступающих по многочисленным *каналам связи* от оборудования пользователей, в сравнительно небольшом количестве узлов *магистральной сети*;
  - ***магистраль (backbone или core network*** - объединяет отдельные *сети доступа*, обеспечивая транзит трафика между ними по высокоскоростным *каналам*;
  - ***информационные центры*** или центры управления сервисами **(data centers или services control point)** - это собственные информационные ресурсы сети, на основе которых осуществляется обслуживание пользователей.

# Сеть доступа

- *Сеть доступа* представляет собой нижний уровень иерархии телекоммуникационной сети.
- К этой сети подключаются конечные (терминальные) узлы – оборудование, установленное у пользователей (абонентов, клиентов) сети. В случае *компьютерной сети* конечными узлами являются компьютеры, телефонной - телефонные аппараты, а *телевизионной* или *радиосети* - соответствующие теле- и радиоприемники.
- Основное назначение *сети доступа* - концентрация информационных потоков, поступающих по многочисленным *каналам связи* от оборудования пользователей, в сравнительно небольшом количестве узлов *магистральной сети*.

# Магистральная сеть

- *Магистральная сеть* объединяет отдельные *сети доступа*, выполняя функции транзита трафика между ними по высокоскоростным *каналам*.
- *Коммутаторы магистрали* могут оперировать не только информационными соединениями между отдельными пользователями, но и агрегированными информационными потоками, переносящими данные большого количества пользовательских соединений. В результате информация с помощью *магистрали* попадает в *сеть доступа* получателей, демультиплексируется там и коммутируется таким образом, что на входной порт оборудования пользователя поступает только та информация, которая ему адресована.
- В том случае, когда абонент-получатель подключен к тому же *коммутатору* доступа, что и абонент-отправитель (непосредственно или через подчиненные по иерархии связей *коммутаторы*), последний выполняет необходимую операцию *коммутации* самостоятельно.

# Информационные центры

- *Информационные центры* (центры управления сервисами) - это собственные информационные ресурсы сети, на основе которых осуществляется обслуживание пользователей. В таких *центрах* может храниться информация двух типов:
  - пользовательская информация, то есть те данные, которые непосредственно интересуют пользователей сети;
  - вспомогательная служебная информация, позволяющая предоставлять пользователям некоторые услуги.

# Информационные центры

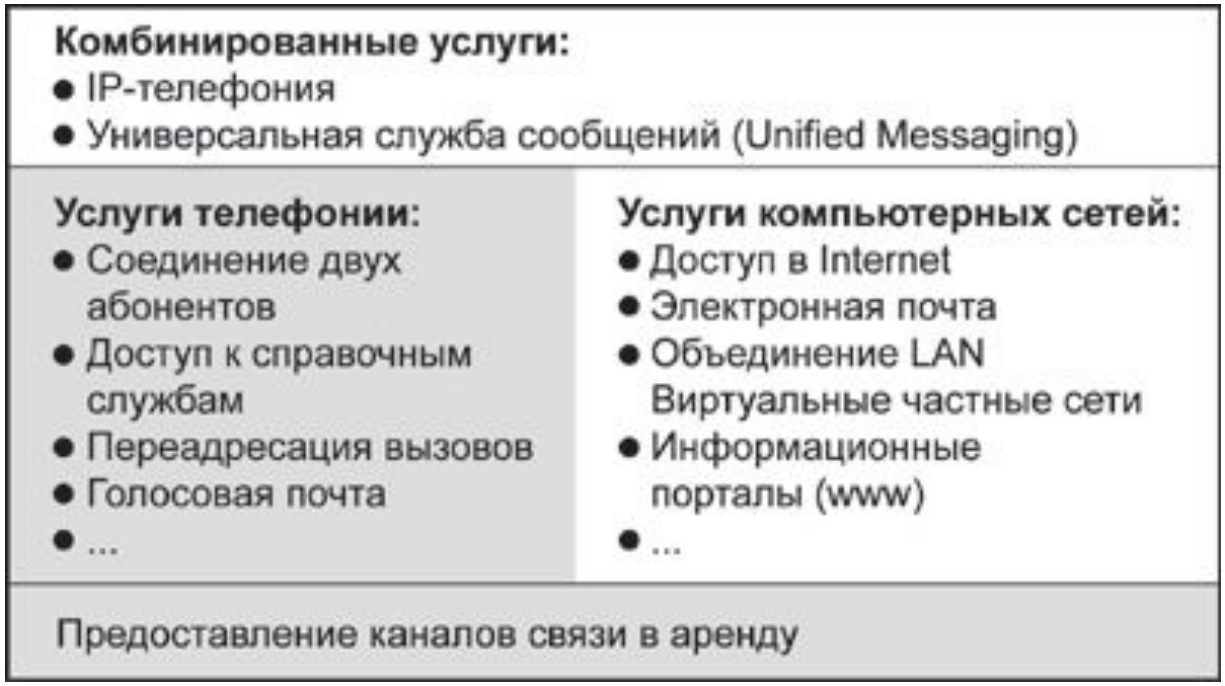
- Примером информационных ресурсов **первого типа** могут служить Web-порталы, на которых расположена разнообразная справочная информация и новости, информация электронных магазинов и т.п.
- К ресурсам **второго типа** относятся, например, различные системы аутентификации и авторизации пользователей, с помощью которых организация, владеющая сетью, проверяет права пользователей на получение тех или иных услуг; системы биллинга, которые в коммерческих сетях подсчитывают плату за предоставленные услуги; базы данных учетной информации пользователей, хранящие имена и пароли, а также перечни услуг, на которые подписан каждый пользователь.
- Еще одним из распространенных видов вспомогательного *информационного центра* является централизованная система управления сетью, которая представляет собой программное обеспечение, работающее на одном или нескольких компьютерах.

# Операторы связи

- Специализированное предприятие, которое создает *телекоммуникационную сеть* для оказания общедоступных услуг, владеет этой сетью и поддерживает ее работу, традиционно называется ***оператором связи (telecommunication carrier)***.
- Операторы связи отличаются друг от друга:
  - набором предоставляемых услуг;
  - территорией, в пределах которой предоставляются услуги;
  - типом клиентов, на которых ориентированы услуги;
  - имеющейся во владении оператора ***инфраструктурой*** - линиями связи, коммутационным оборудованием, информационными серверами и т.п.

# Услуги, провайдеры услуг и сетевая инфраструктура

- Операторы связи осуществляют свою деятельность на коммерческой основе, заключая договоры с потребителями услуг.
- Классификация примерных услуг представлена на рисунке.



# Услуги провайдеров

- Услуги можно классифицировать в зависимости от того, предоставляется ли клиенту дополнительная информация:
  - услуги, состоящие в передаче трафика в неизменном виде между абонентами сети;
  - услуги, состоящие в предоставлении пользователю информации, созданной оператором или операторами связи.
- Телефонный разговор - это пример услуги первого типа, так как информация создается абонентами сети, а оператор только доставляет ее от одного абонента к другому. К этому же типу относится услуга соединения двух локальных сетей клиента с помощью сети передачи данных оператора.
- Примерами услуг второго типа (их обычно называют информационными) являются услуги справочных служб *телефонной сети* или услуги какого-либо Web-сайта.

# Лицензирование услуг

- Каждый оператор связи оказывает те услуги из общего набора, которые ему представляются наиболее соответствующими его профилю и экономически выгодными.
- В большинстве стран мира (в том числе, в России) операторы связи должны получать от государственных органов **лицензии** на оказание тех или иных услуг связи.
- Практически во всех странах имеются операторы, которые фактически являются монополистами на рынке телекоммуникационных услуг в масштабах страны.
- Сегодня происходит процесс демонополизации этой области деятельности.

# Клиенты

- Все множество клиентов – потребителей инфотелекоммуникационных услуг – можно разделить на две больших категории:
  - массовые индивидуальные клиенты;
  - корпоративные клиенты.

# Массовые индивидуальные клиенты

- Для массовых клиентов очень важна экономичность услуги - низкая месячная оплата, возможность использования стандартных терминальных устройств (телефонные аппараты, телевизионные приемники, персональные компьютеры), а также существующей в квартире проводки в виде телефонной пары и телевизионного коаксиального кабеля.
- Традиционная в домах проводка - это серьезное ограничение для предоставления услуг доступа в Internet и новых услуг *компьютерных сетей*, так как она не рассчитана на передачу данных, а подведение к каждому дому нового качественного кабеля, например, волоконно-оптического, обойдется недешево.
- Поэтому доступ в Internet часто осуществляется с помощью низкоскоростного модемного соединения по *телефонной сети*.
- Однако постепенно развиваются новые технологии (ADSL и др.) - так называемые технологии цифровых абонентских линий, позволяющие передавать по существующей телефонной проводке данные с гораздо более высокой скоростью, чем обычные модемы.

# Корпоративные клиенты

- Корпоративные клиенты - это предприятия и организации различного профиля.
- Небольшие предприятия по набору предпочтительных услуг не слишком отличаются от массовых клиентов и потребности в передаче данных сводится к стандартному модемному доступу к Internet.
- Крупные предприятия, состоящие из нескольких территориально рассредоточенных отделений и филиалов, а также имеющие сотрудников, работающих вне офиса, нуждаются в расширенном наборе услуг.
- Прежде всего, такой услугой является виртуальная частная сеть (Virtual Private Network, VPN. Услуги VPN могут предоставляться как для телефонии (например, корпоративные пользователи звонят по сокращенным внутренним номерам), так и для сетей передачи данных.

# Электронная почта

- Электронная почта – важное средство обмена информацией в современном мире.
- Существует несколько сетевых протоколов используемых для приема-передачи, а также управления почтовыми сообщениями:
  - smtp
  - pop3
  - imap
- Обмен электронными почтовыми сообщениями основан на использовании клиент-серверной архитектуры, где почтовые серверы играют роль компьютеров, осуществляющих получение, хранение и доставку почты по запросам пользователей.

# Типы почтовых серверов

- Для централизованного управления почтовыми сообщениями используются специализированные компьютеры – **почтовые серверы**.
- **Почтовыми серверами** также называют специализированное программное обеспечение, выполняющее необходимые функции обслуживания почтовых клиентов, приема и передачи почтовых сообщений.
- На сервере может быть запущены модули поддержки нескольких почтовых протоколов:
  - протоколы принудительной доставки (передача почты инициируется отправителем);
  - протоколы доставки по запросу (передача инициируется получателем сообщения).

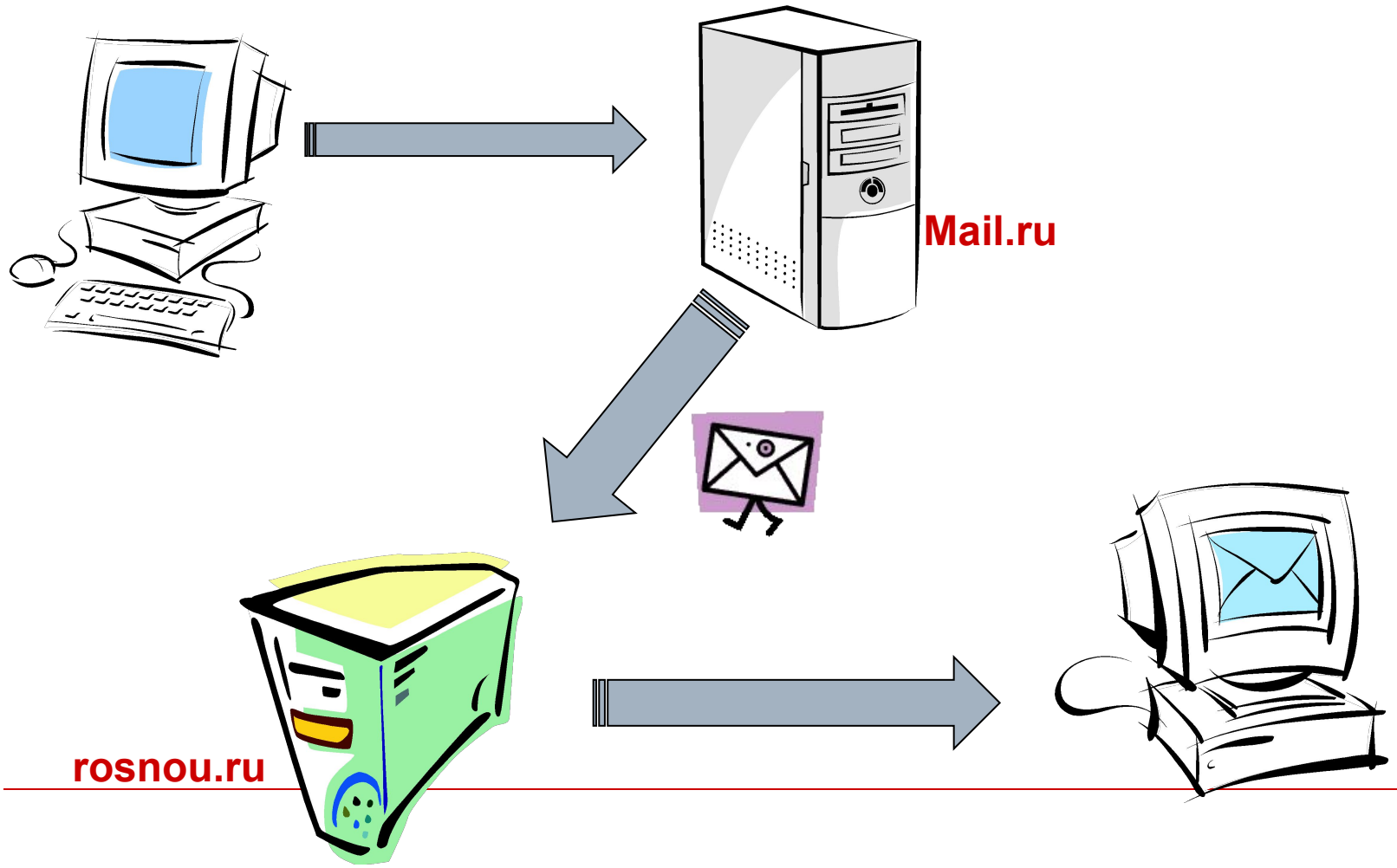
# Протоколы принудительной доставки почты

- Почтовые серверы могут отправлять почту не только между пользователями одного компьютера, но и на другие компьютеры. Для таких процессов используются **ретрансляторы почты** – система, принимающая почту от одного компьютера и посылающая на другой.
- В качестве протокола принудительной доставки почтовых сообщений обычно выступает протокол SMTP (Simple Mail Transport Protocol).
- Важная особенность при работе такого протокола – компьютер-получатель должен быть доступен.

# Серверы доставки по запросу

- Последнее звено в цепи доставки почты обычно составляют серверы доставки по запросу.
- Наиболее популярные протоколы данного класса – POP (Post Office Protocol), IMAP (Internet Message Access Protocol).
- Данные протоколы используются, когда конечным получателем является рабочая станция, на которой не запущен сервер принудительной доставки.

# Процесс доставки почтовых сообщений



# Серверы принудительной доставки почты

- Серверы принудительной доставки почты – важнейший компонент в системе обмена электронной почты.
- Для UNIX систем примерами могут служит следующие популярные почтовые сервера:
  - sendmail;
  - qmail;
  - exim;
  - postfix
- Для Windows систем можно использовать специализированные серверы (такие как Exchange) или службу SMTP, входящую в состав IIS, службу pop3, входящую в состав Windows Server 2003 R2.

# Служба SMTP в Windows

- В IIS 6 входит служба простого протокола электронной почты (SMTP).
- Средства администрирования IIS позволяют сконфигурировать SMTP-сервер для распространения служб обмена сообщениями на разнообразные платформы.
- При пересылке сообщения SMTP-сервер вначале устанавливает соединение с ближайшим узлом.
- Если это соединение не установлено или по каким-либо причинам недоступно, SMTP-сервер отклоняет прием сообщения от клиента и уведомляет его об ошибке.
- По умолчанию SMTP-сервер напрямую соединяется с сервером, на котором находится домен-получатель сообщения.

# Параметры конфигурации

- При работе с SMTP-сервером администратор должен контролировать следующие параметры:
  - Аутентификацию клиентов на SMTP-сервере перед отправкой сообщения;
  - Передачу сообщений клиента на SMTP-сервер;
  - Отправку сообщений с SMTP-сервера;
  - Маршрутизацию сообщений с SMTP-сервера;
  - Настройки SMTP для заданного домена SMTP.