ИНФОРМАТИКА
Часть 3

Зобнин Юрий Александрович
кандидат социологических наук
доцент кафедры бизнес-информатики и математики
каб. 519 (7-й корп. ТИУ)
greentree1959@mail.ru

Компьютерные сети

Компьютерная сеть – совокупность компьютеров, объединенных каналами передачи данных для обмена информацией и коллективного использования аппаратных, программных и информационных ресурсов сети.

Любая ЭВМ обладает тремя видами ресурсов: информационным, техническим и программным. Технический потенциал, кроме того, может быть увеличен за счет подключаемых устройств – принтеров, сканеров, внешней памяти и др.

Соединение компьютеров в сеть позволяет объединить разрозненные ресурсы и получить в пользование каждым участником суммарный объем сетевых ресурсов, многократно более мощный.

Ресурсы компьютерных сетей

Информационные – базы данных общего и индивидуального применения, ориентированные на решаемые в сети задачи

Аппаратные – компьютеры различных типов, средства территориальных систем связи, аппаратура связи и согласования работы сетей одного и того же уровня или различных уровней (hardware)

Программные – комплекс программ для планирования, организации и осуществления коллективного доступа пользователей к общественным ресурсам, автоматизации обработки информации, динамического распределения и перераспределения общесетевых ресурсов с целью повышения оперативности и надежности удовлетворения запросов пользователей (software)

Таким образом, компьютерная сеть состоит из некоторого количества компьютеров с их индивидуальными ресурсами, а также – каналов связи этих компьютеров между собой. Кроме того, сеть может быть наделена ресурсами коллективного пользования, например: сетевой принтер, сетевая вычислительная машина, сетевая база данных, сетевой набор определенных программ и др.

И наконец, для обеспечения надлежащего взаимодействия включенных в сеть компьютеров и их программного обеспечения, бесперебойной передачи данных, распределения ресурсов сети между ее участниками необходимы сетевое оборудование, сетевые программные средства и единые стандарты работы в сети.

КОМПЬЮТЕРНАЯ СЕТЬ					
Компьютеры с их индиви-дуальными ресурсами (программны-ми, информа-ционными, и техническими)	**Каналы связи** между компьютерами, прочими устройствами (проводные, беспроводные)	**Коллективные ресурсы сети** (базы данных, программы, компьютеры, прочие устройства)	**Сетевое программное обеспечение** (специальные программные средства, например, операционные системы Unix, NetWare, Windows-NT и др.)	**Сетевое оборудование** и устройства (специальное аппаратное (техническое) обеспечение например, сетевая карта, модем и др.)	**Сетевые протоколы** (правила, стандарты передачи данных, другого взаимодей-ствия компьютеров и программ)

Классификации компьютерных сетей

1. По территориальной распространенности:

- локальные сети - связывают пользователей одного или нескольких офисов либо кабинетов одного предприятия, а также - дома, подъезда, квартиры;
- глобальные сети - объединяют пользователей, расположенных по всему миру (с использованием, в т.ч., спутниковых каналов связи: 10-15 тыс. км);
- региональные сети - объединяют пользователей города, области, небольших стран (в качестве каналов связи обычно используются телефонные кабели: 10-1000 км);
- корпоративные сети - связывают пользователей крупных организаций, в т.ч., глобальных компаний.

2. По типу среды передачи:

- на базе коаксиального кабеля;
- на базе витой пары;
- на базе оптико-волоконного кабеля;
- на базе радиоканалов;
- на базе инфракрасного излучения.

3. По скорости передачи информации:

- низкоскоростные;
- среднескоростные;
- высокоскоростные.

4. По принадлежности:

- ведомственные;
- государственные;
- частные;
- общественные.

5. По организации взаимодействия:

6. По цели деятельности:

ЛОКАЛЬНЫЕ СЕТИ ЭВМ

Локальная компьютерная сеть имеет и другие названия: локальная сеть ЭВМ, локальная вычислительная сеть (ЛВС), Local Area Network (LAN).

Обычно ЛВС покрывает относительно небольшую территорию или небольшую группу зданий, помещений. Однако существуют локальные сети, узлы которых разнесены географически на расстояния более 12 тыс. км, например, космические станции и орбитальные центры.

В любом случае, ЛВС – это компьютерная сеть, имеющая физические и/или логические границы.

Чаще всего локальные сети подразделяют на одноранговые и иерархические .

В одноранговых сетях любой пользователь сети может получить доступ к данным, хранящимся на любом компьютере.

Достоинства одноранговых сетей:

- наиболее просты в установке и эксплуатации.
- операционные системы типа Windows обладают всеми необходимыми функциями, позволяющими строить одноранговую сеть.

Недостатком одноранговых сетей является затрудненность в решении вопросов защиты информации. Поэтому такой способ организации сети используется для сетей с небольшим количеством компьютеров и там, где вопрос защиты данных не является принципиальным.

В иерархической сети при установке сети заранее выделяются один или несколько специальных компьютеров, называемых серверами. Им вменяется выполнение двух особых функций:

- управление обменом данных по сети;
- распределение ресурсов сети (информационных, программных, аппаратных).

Иерархическая модель сети является наиболее предпочтительной, так как позволяет создать наиболее устойчивую структуру сети и более рационально распределить ресурсы. Другим достоинством иерархической сети является более высокий уровень защиты данных.

К недостаткам иерархической сети, по сравнению с одноранговыми сетями, относятся:

- необходимость дополнительной ОС для сервера.
- более высокая сложность установки и модернизации сети.
- необходимость выделения отдельного компьютера в качестве сервера.
- более высокие материальные затраты на создание и функционирование сети.

Рабочая станция (PC) - это подключенный к сети персональный компьютер, на котором пользователь сети выполняет свою работу. Каждая PC обрабатывает свои локальные файлы и использует свою ОС. Но при этом пользователю доступны ресурсы сети. Различают три типа PC:

- с локальным диском (ОС загружается с локального диска),
- бездисковая (ОС загружается с диска файлового сервера - обеспечивается с помощью специальной микросхемы сетевого адаптера),
- удаленная (подключается через телекоммуникационные каналы связи - с помощью телефонной сети).

Сервер сети - это компьютер, подключенный к сети и предоставляющий пользователям сети определенные услуги, выполняющий функции по обслуживанию клиента: в частности, сервер распределяет пользователям ресурсы сети: принтеры, внешнюю память, базы данных, программы и т. д. Сервер может предоставлять участникам сети и свои собственные ресурсы – технические, информационные, программные.

Поэтому серверы, как правило, представляют из себя высокопроизводительные компьютеры, нередко - с несколькими параллельно работающими процессорами, с лучшими по сравнению с клиентом техническими характеристиками, такими как быстродействие, объем дисковой памяти, объем оперативной памяти и др.

Технологии использования сервера

В компьютерных сетях используются распределённые (distributed) технологии: все компоненты системы распределены по нескольким компьютерам.

Различают две распределенных технологии использования сервера:

- **файл-серверная технология** - база данных находится на файловом сервере, а СУБД и клиентские приложения находятся на рабочих станциях;
- **клиент-серверная технология** - на сервере находится и база данных, и СУБД, а на рабочих станциях находятся только клиентские приложения.

ФАЙЛОВЫЙ СЕРВЕР

выполняет функции хранения данных и предоставления доступа к ним

- хранение данных;
- архивирование данных;
- согласование изменений, выполняемых разными пользователями;
- передача данных;
- обеспечение доступа пользователей к хранимым данным;
- обеспечение одновременного доступа многих пользователей к общим данным.

СЕРВЕР БАЗ ДАННЫХ

выполняет функции хранения, обработки и управления файлами баз данных (БД)

- хранение БД, поддержка их целостности, полноты, актуальности;
- прием и обработка запросов к БД, а также пересылка результатов обработки на РС;
- обеспечение авторизированного доступа к БД, поддержка системы ведения и учета пользователей, разграничение прав доступа пользователей;
- согласование изменений данных, выполняемых разными пользователями одновременно;
- поддержка распределенных баз данных, взаимодействие с иными серверами БД, расположенными в других местах.

В системах с технологией «файл-сервер» подавляющее большинство программ и данных хранится на файловом сервере. По запросу пользователя сервер пересылает ему необходимые программы и данные. Затем на рабочей станции (у пользователя) выполняется обработка информации.

Файловый сервер, таким образом, осуществляет только файловые операции ввода-вывода и хранит файлы любого типа. Для обеспечения бесперебойной работы и повышенной скорости записи и чтения данных файловый сервер, как правило, обладает большим объемом дискового пространства.

Достоинства технологии «файл-сервер»: требуется относительно небольшое время для создания ПО при минимальных затратах на разработку, обновление и изменения.

Недостатки: 1) необходимость ограничения числа клиентов, одновременно работающих с базой данных для контролирования объёма трафика и нагрузок на сети передачи данных, а также – актуальности БД; 2) высокие затраты на модернизацию и сопровождение сервисов на каждой клиентской рабочей станции.

В системах с технологией «клиент-сервер» хранение данных и их обработка производится на мощном сервере, который выполняет также контроль доступа к ресурсам и данным. Рабочая станция направляет серверу запросы и получает результаты их обработки сервером.

Таким образом, в клиент-серверных системах функционируют (взаимодействуют) два звена (*two-tier*): приложение-сервер (СУБД, back-end) и клиентские приложения (front-end): обмен данными осуществляется на уровне программ. То есть, рабочие станции, на которых находятся клиентские приложения, обращаются напрямую к серверу баз данных, на котором находится СУБД.

Существуют и многозвенные (*multi-tier*) клиент-серверные технологии. В качестве промежуточных звеньев выступают так называемые серверы приложений (*application servers*). В таких системах пользовательские клиентские приложения обращаются к СУБД не напрямую, а через это промежуточное звено. Типичный пример многозвенности — современные веб-приложения, использующие базы данных. В таких приложениях помимо звена СУБД и клиентского звена, выполняющегося в веб-браузере, имеется как минимум одно промежуточное звено — веб-сервер с соответствующим серверным программным

Многозвенность позволяет более эффективно использовать возможности серверов и клиентов, благодаря разделению функций хранения, обработки, представления данных и вынесения их на один или несколько отдельных серверов.

Таким образом, в технологиях «клиент-сервер» в соответствии с тем, как распределены задания или сетевая нагрузка между компьютерами иерархической сети, все ее участники делятся на две группы:

- основные участники - заказчики услуг, называемые **клиентами;**
- вспомогательные участники - поставщики услуг, называемые **серверами**.

Сам сервер может быть клиентом другого сервера, но только более высокого уровня иерархии. Поэтому иерархические сети иногда называются сетями с выделенным сервером.

Клиентами и серверами называются не только аппаратные средства, но также и взаимодействующие приложения (программы). В таком смысле клиент – это приложение, отвечающее за обработку, вывод информации и передачу запросов к серверу (программе).

Преимущества технологии «клиент-сервер»:

- поскольку все вычисления выполняются на сервере, то требования к компьютерам, на которых установлен клиент, снижаются (рабочая станция = машина запросов).
- поскольку все данные хранятся на одном компьютере (сервере), а не на рабочих станциях, то можно гораздо надежнее и эффективнее обеспечить контроль полномочий, учет прав доступа клиентов и в целом безопасность и защищенность систем и данных.

Недостатки:

- неработоспособность сервера может сделать неработоспособной всю вычислительную сеть (сервер признается неработоспособным, если его производительности не хватает на обслуживание всех клиентов, если он находится на профилактике, ремонте и т. п.);
- поддержка системы требует отдельного специалиста — системного администратора;
- высокая стоимость как самого оборудования, так и его поддержки.

Кроме серверов и рабочих станций в компьютерных сетях выделяются также специальные **коммуникационные узлы**, обеспечивающие обмен данными между элементами сети.

Коммуникационные устройства могут быть как специализированными, так и универсальными (комбинированными) в различной степени.

В узлах мощных сетей используются уже так называемые коммутационные машины (ЭВМ).

Коммуникационные узлы сети

ПОВТОРИТЕЛЬ	**МОСТ**	**МАРШРУТИЗАТОР**	**ШЛЮЗ**
(концентратор, repeater, хаб, hub)	(коммутатор, bridge)	(роутер, router)	(gateway)
- устройство, усиливающее или регенерирующее пришедший на него сигнал.	- устройство, выполняющее развязку, присоединенных к нему сегментов.	- устройство, соединяющее сети одного или разных типов по одному протоколу обмена данными.	- устройство, позволяющее организовать обмен данными между разными сетевыми объектами.
Повторитель, приняв пакет из одного сегмента сети, передает его во все остальные, т. е. поддерживает обмен данными только между двумя станциями одного или разных сегментов	Мост одновременно поддерживает несколько процессов обмена данными для каждой пары станций разных сегментов	Маршрутизатор анализирует адрес назначения и направляет данные по оптимально выбранному маршруту	Шлюз служит для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной сетей).

Современные персональные компьютеры обладают всем необходимым для организации небольшой локальной компьютерной сети – полным набором программ и устройств. С помощью сервиса «Мастер установки/настройки сети» пользователь имеет возможность быстро организовать, например, домашнюю (семейную) локальную компьютерную сеть.

Для построения простой локальной сети используются маршрутизаторы, коммутаторы, точки беспроводного доступа, беспроводные маршрутизаторы, модемы и сетевые адаптеры (сетевые карты). Реже используются преобразователи (конвертеры) среды, усилители сигнала (повторители разного рода) и специальные антенны.

Модем - устройство, необходимое для организации связи между компьютерами, обычно с использованием телефонных каналов.

Модем выполняет функции модуляции и демодуляции информационных сигналов, то есть преобразования входных аналоговых сигналов телефонной линии в цифровые биты и наоборот. Основной характеристикой модема является скорость передачи данных (бит в секунду).

По способу подключения различают модемы:

- внешние - подключаются к разъему последовательного порта, выведенному на заднюю стенку системного блока);
- внутренние - устанавливаются в один из разъемов материнской платы.

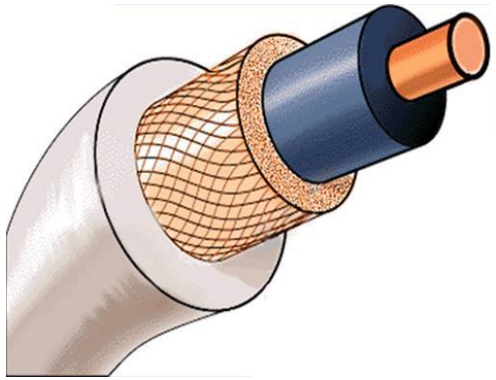
Отдельная локальная вычислительная сеть может иметь связь с другими локальными сетями через шлюзы, а также быть частью глобальной вычислительной сети (например, Интернет) или иметь подключение к ней.

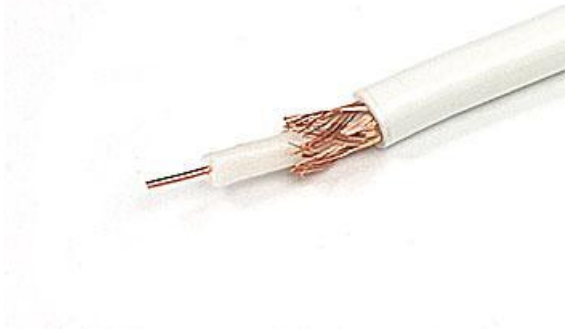
Нередко в локальной сети организуют **рабочие группы** — формальное объединение нескольких компьютеров в условную подсеть со своим наименованием.

Для физического соединения компьютеров в сеть используются различные среды доступа: проводные металлические, оптические проводники) и беспроводные технологии (радиоканал). Проводные связи обычно построены на технологиях **Ethernet**, беспроводные - **Wi-Fi**, Bluetooth, GPRS.

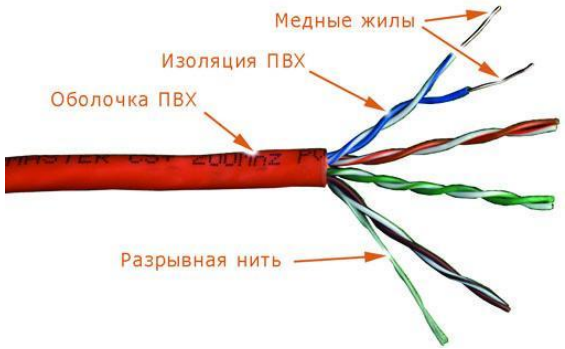
Наиболее распространенными в использовании остаются **кабельные линии связи** как физическая среда для передачи данных**.** Кабель представляет собой один или несколько проводников, помещенных в изолирующие материалы. Используются три вида кабелей: коаксиальный, витая пара, оптико-волоконный.

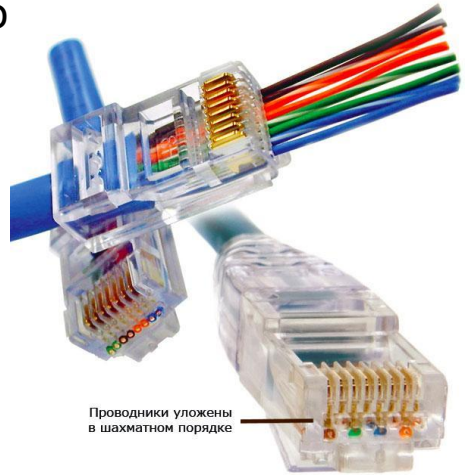
В центре **коаксиального кабеля** находится жесткий медный проводник, окруженный толстым слоем изоляционного материала. Второй проводник сделан в виде оплетки поверх изоляции. Весь кабель помещается во внешнюю пластиковую оболочку.



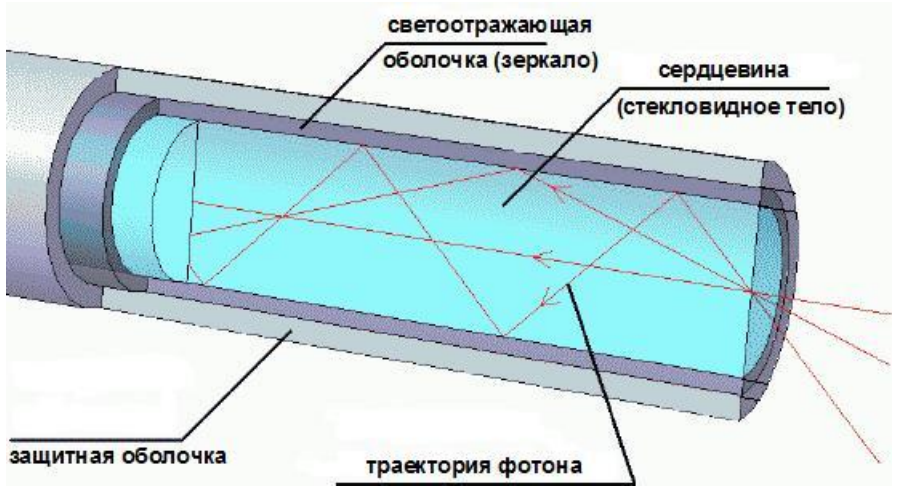


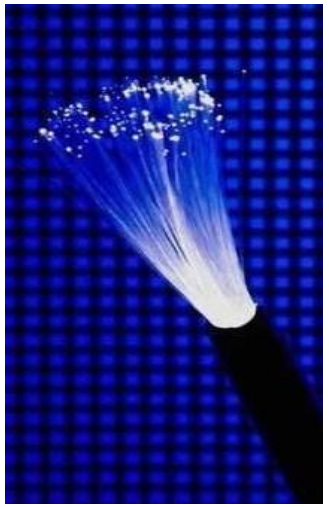
Кабель витой пары состоит из двух проводников, заключенных в оболочку. Для уменьшения влияния помех проводники скручиваются с определенным шаго





В **оптико-волоконном кабеле** для передачи данных используются световые импульсы. Сердечник такого кабеля изготовлен из стекла или пластика. Сердечник окружен слоем отражателя, который направляет световые импульсы вдоль кабеля. Такой кабель не подвержен воздействию электромагнитных полей.

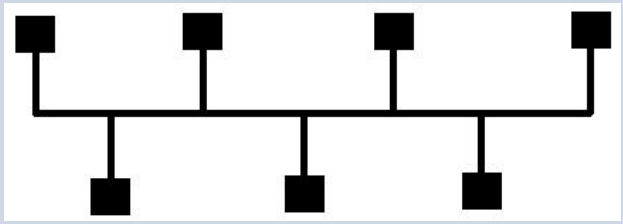
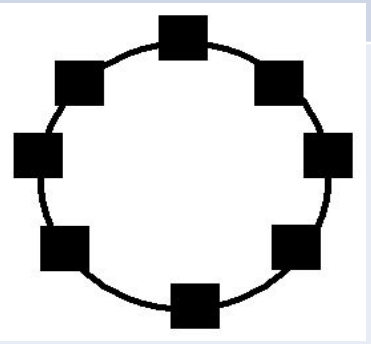
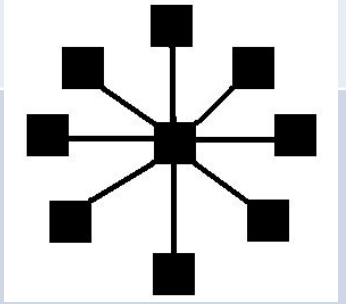




ТОПОЛОГИЯ СЕТИ - схема соединений узлов компьютерной сети.
Узел сети - компьютер либо коммутирующее устройство сети (коммуникационный узел).
Ветвь (ребро) сети - это путь, соединяющий два смежных узла.
Топологии делятся на:

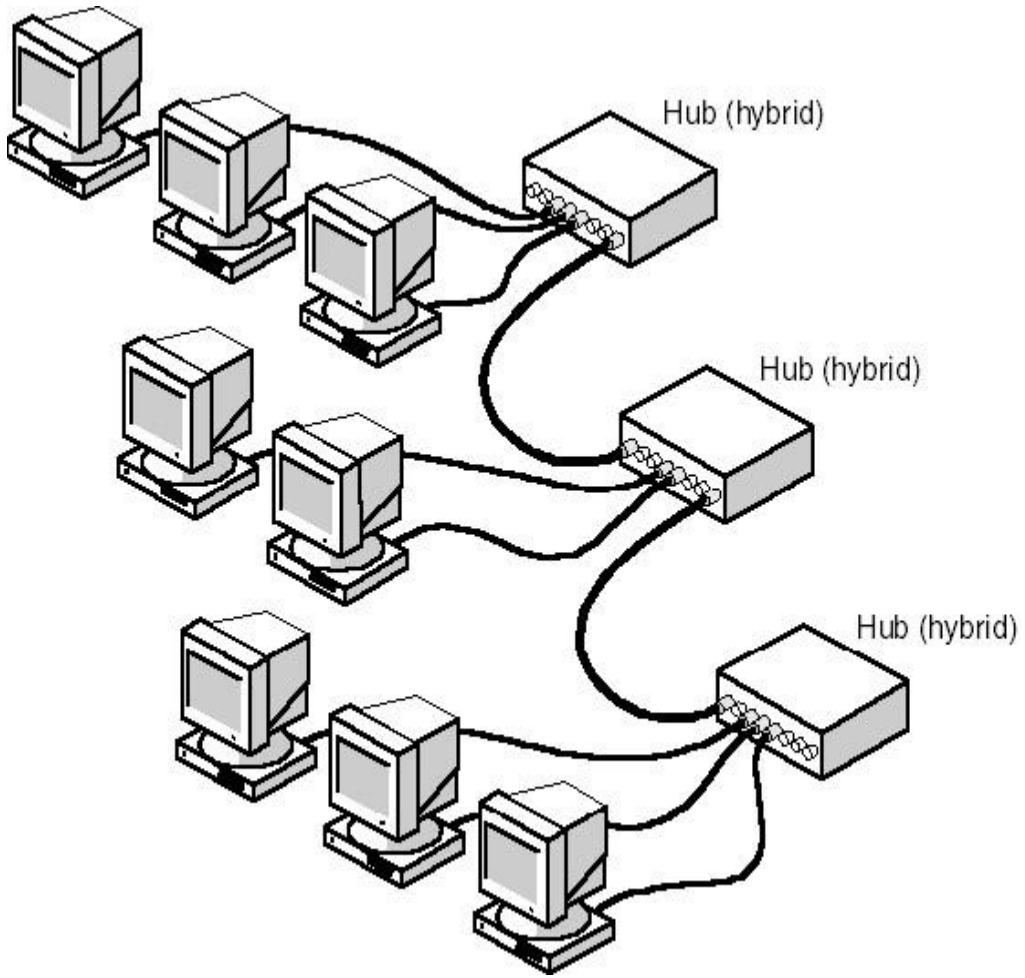
- полносвязные - каждый компьютер сети связан со всеми остальными. На практике этот вариант используется в настоящее время очень редко, так является громоздким и эффективным;
- неполносвязные — не имеется непосредственной линии связи между всеми компьютерами, а для обмена данными между двумя компьютерами используется промежуточная передача

Базовые топологии локальных сетей

Наименование топологии, характеристика	Схематическое изображение
Шина (bus) - компьютеры подключаются к одному кабелю; - информация передается в обе стороны; - преимущества: простота организации, низкая стоимость; - недостатки: низкая устойчивость к повреждениям (при обрыве в одном месте перестает работать вся сеть).	
Кольцо (ring) - информация передается в одну сторону; - активно применяется фирмой IBM (сети Token Ring); - преимущество: высокая надежность (за счет избыточности); - недостаток: высокая стоимость из-за большого количества адаптеров и дополнительных приспособлений.	
Звезда (star) - каждый компьютер подключается отдельным кабелем к общему устройству (концентратору, хабу), который находится в центре сети; - преимущество: надежность (при обрыве кабеля перестает работать только один компьютер);	

Комбинированные топологии

Звезда - Шина



Звезда - Кольцо

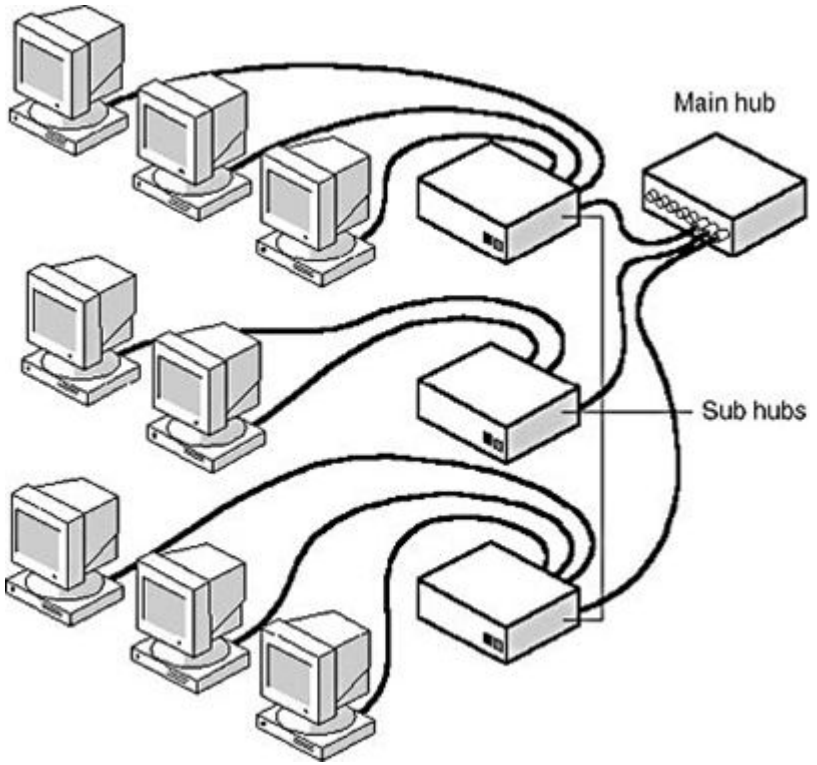
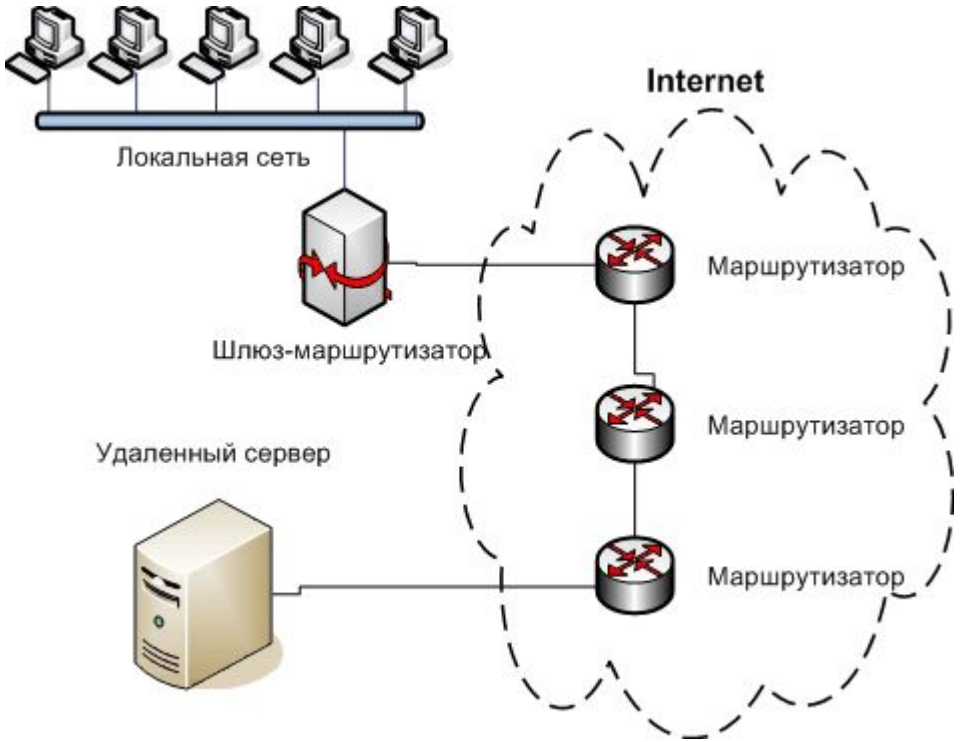


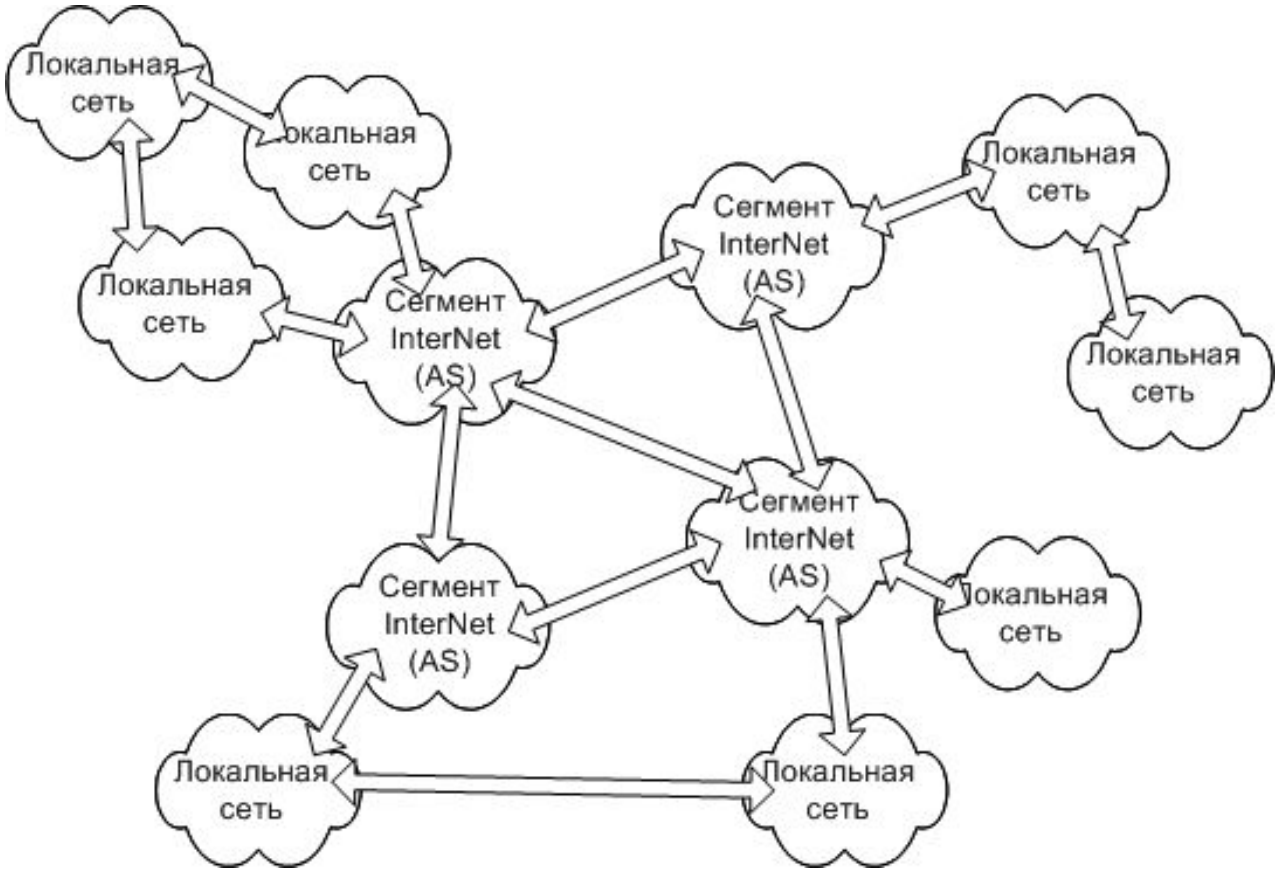
Схема прохождения пакетов из локальной сети к серверу



Все наши компьютеры объединены в локальную сеть, и имеют локальную IP-адресацию. Пакеты с такой адресацией "путешествовать" в глобальной сети не смогут, т.к. маршрутизаторы их не пропустят. Поэтому существует шлюз, который преобразовывает пакеты с локальными IP-адресами, давая им свой внешний адрес.

Маршрутизаторы объединяют отдельные сети в общую составную сеть. К каждому маршрутизатору могут быть присоединены несколько сетей. **Маршрут** - это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до

Схема объединения отдельных сетей в общую составную сеть



Локальных сетей слишком много, поэтому на практике объединяют так называемые автономные системы.

Автономная система (AS - autonomous system) - это сеть, находящаяся под одним административным контролем. АС - понятие достаточно условное: это может быть несколько компьютеров или большая сеть.

Сетевая модель OSI

Основная задача при разработке и эксплуатации сетей – согласование взаимодействия ЭВМ клиентов, серверов, линий связи и других устройств. Она решается путем установления определенных правил, называемых **протоколами.** Часть протоколов реализуется программно, часть – аппаратно.

Для единого представления данных в линиях связи, по которым передается информация, Международная организация по стандартизации (ISO – International Standards Organization) разработала модель международного коммуникационного протокола, в рамках которой разрабатываются различные международные стандарты

Сетевая модель OSI (англ. open systems interconnection basic reference model — базовая Эталонная модель взаимодействия открытых систем, сокр. ЭМВОС; 1978 г.) — абстрактная сетевая модель для коммуникаций и разработки сетевых протоколов.

Модель предлагает взгляд на компьютерную сеть с точки зрения измерений. Каждое измерение обслуживает свою часть процесса взаимодействия. Благодаря такой структуре совместная работа сетевого оборудования и программного обеспечения становится гораздо проще и прозрачнее.

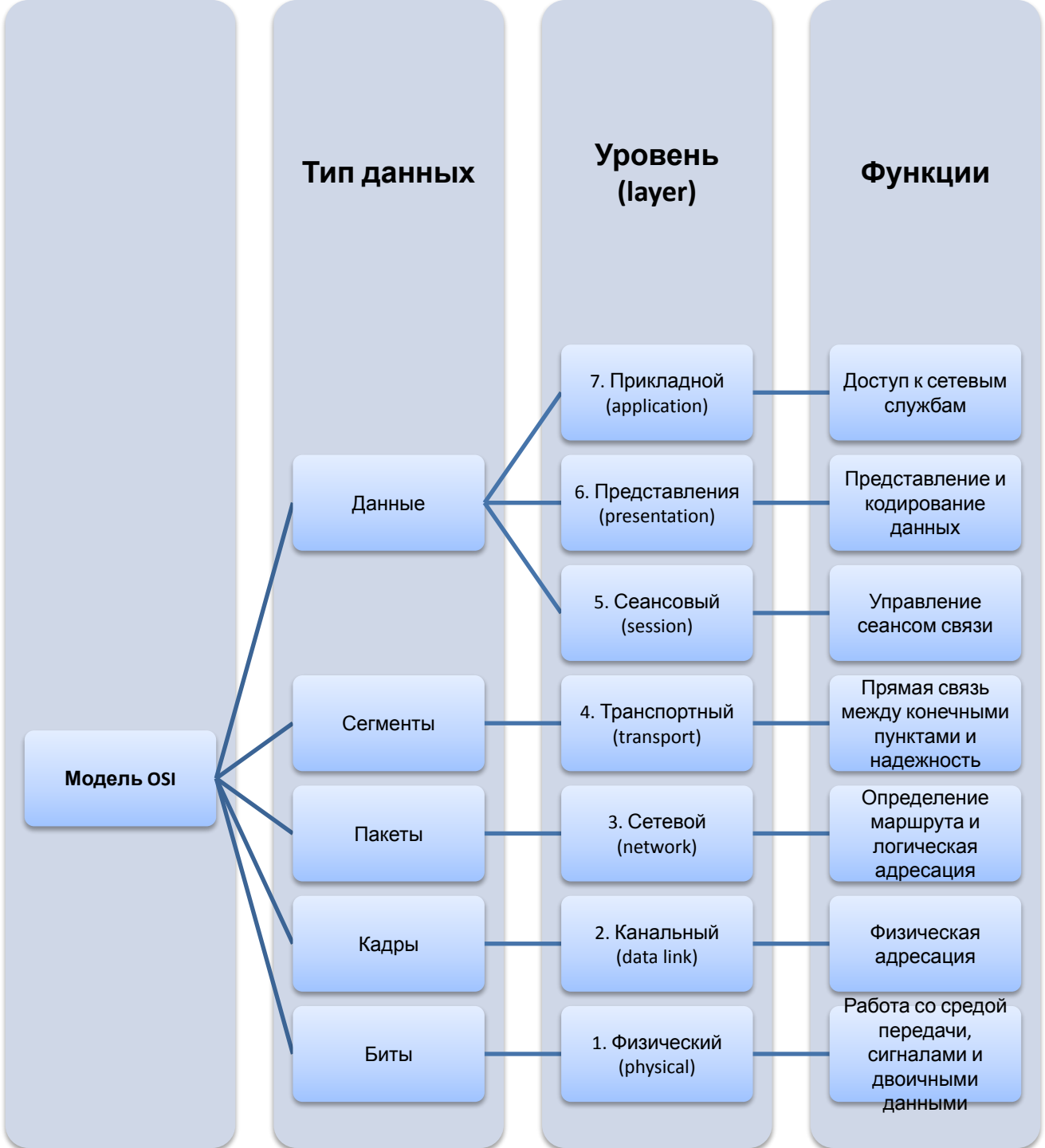
В литературе наиболее часто принято начинать описание уровней модели OSI с 7-го уровня, называемого прикладным, на котором пользовательские приложения обращаются к сети.

Модель OSI заканчивается 1-м уровнем — физическим, на котором определены стандарты, предъявляемые независимыми производителями к средам передачи данных:

- тип передающей среды (медный кабель, оптоволокно, радиоэфир и др.),
- тип модуляции сигнала,
- сигнальные уровни логических дискретных состояний (нуля и единицы).

Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня.

Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на


Модель OSI
Тип данных
Данные
Сегменты
Пакеты
Кадры
Биты
Уровень (layer)
7. Прикладной (application)
6. Представления (presentation)
5. Сеансовый (session)
4. Транспортный (transport)
3. Сетевой (network)
2. Канальный (data link)
1. Физический (physical)
Функции
Доступ к сетевым службам
Представление и кодирование данных
Управление сеансом связи
Прямая связь между конечными пунктами и надежность
Определение маршрута и логическая адресация
Физическая адресация
Работа со средой передачи, сигналами и двоичными данными

Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня, что не выполняется в протоколах альтернативных моделей.

Каждому уровню с некоторой долей условности соответствует свой операнд — логически неделимый элемент данных, которым на отдельном уровне можно оперировать в рамках модели и используемых протоколов: на физическом уровне мельчайшая единица — бит, на канальном уровне информация объединена в кадры, на сетевом — в пакеты (датаграммы), на транспортном — в сегменты.

Любой фрагмент данных, логически объединённых для передачи — кадр, пакет, датаграмма — считается сообщением. Именно сообщения в общем виде являются операндами сеансового, представительского и прикладного уровней.

К базовым сетевым технологиям относятся физический и канальный уровни.

Физический, канальный и в некоторых случаях сетевой уровень являются сетезависимыми, т. е. тесно связаны с коммуникационным оборудованием. Сеансовый, представления данных, прикладной уровень являются сетенезависимыми. Транспортный и сетевой являются промежуточными.

Наряду с коммуникационными процессами в сети выделяются еще два вида процессов, протекающих в сети: информационные и транспортные.

Информационные процессы определяются тремя верхними уровнями сетевой архитектуры (прикладным уровнем, уровнем представления данных и сеансовым) и занимаются представлением информации для пользователя.

Транспортные процессы поддерживаются транспортным уровнем, определяющим процедуры и формы передачи информации от одной системы к другой. Именно протоколы семейства TP (Transport Protocol) обеспечивают надежную передачу и доставку блоков информации адресатам и управляют этой доставкой.

Для запоминания названий 7-и уровней модели OSI на английском языке рекомендуют использовать фразу "All People Seem To Need Data Processing", в которой первые буквы слов соответствуют первым буквам названий уровней. Для запоминания уровней на русском

- **Прикладной уровень (7)**

Прикладной уровень (уровень приложений; англ. application layer) — верхний уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью:

- позволяет приложениям использовать сетевые службы (удалённый доступ к файлам и базам данных,

пересылка электронной почты);

- отвечает за передачу служебной информации;
- предоставляет приложениям информацию об ошибках;
- формирует запросы к уровню представления.

Протоколы прикладного уровня: HTTP, POP3, FTP, XMPP, OSCAR, Modbus, SIP, TELNET.

- **Представительский уровень (6)**

Представительский уровень (уровень представления; англ. presentation layer) обеспечивает преобразование протоколов, а также кодирование и декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

Уровень представлений обычно представляет собой промежуточный протокол для преобразования информации из соседних уровней. Это позволяет осуществлять обмен между приложениями на разнородных компьютерных системах прозрачным для приложений образом. Уровень представлений обеспечивает форматирование и преобразование кода. Форматирование кода используется для того, чтобы гарантировать приложению поступление информации для обработки, которая имела бы для него смысл. При необходимости этот уровень может выполнять перевод из одного формата данных в другой.

Уровень представлений имеет дело не только с форматами и представлением данных, но

Чтобы понять, как это работает, представим, что имеются две системы. Одна использует для представления данных расширенный двоичный код обмена информацией EBCDIC. Например, это может быть мейнфрейм компании IBM. Напротив, другая использует американский стандартный код обмена информацией ASCII (его используют большинство других производителей компьютеров). Если этим двум системам необходимо обменяться информацией, то нужен уровень представлений, который выполнит преобразование и осуществит перевод между двумя различными форматами.

Еще одной функцией, выполняемой на уровне представлений, является шифрование данных, которое применяется в тех случаях, когда необходимо защитить передаваемую информацию от приема несанкционированными получателями. Чтобы решить эту задачу, процессы и коды, находящиеся на уровне представлений, должны выполнить преобразование данных. На этом уровне существуют и другие подпрограммы, которые сжимают тексты и преобразовывают графические изображения в битовые потоки так, что они могут передаваться по сети.

Стандарты уровня представлений также определяют способы представления графических изображений. Для этих целей может использоваться формат PICT — формат изображений, применяемый для передачи графики QuickDraw между программами.

Другим форматом представлений является тэгированный формат файлов изображений TIFF, который обычно используется для растровых изображений с высоким разрешением. Следующим стандартом уровня представлений, который может использоваться для графических изображений, является стандарт, разработанный Объединенной экспертной группой по фотографии (Joint Photographic Expert Group), в повседневном пользовании известный как JPEG.

Существует и другая группа стандартов уровня представлений, которая определяет представление звука и кинофрагментов. Сюда входят:

- интерфейс электронных музыкальных инструментов (англ. Musical Instrument Digital Interface – MIDI) для цифрового представления музыки;
- стандарт MPEG, разработанный Экспертной группой по кинематографии и используемый

- стандарт QuickTime, описывающий звуковые и видео элементы для программ, выполняемых на компьютерах Macintosh и PowerPC.

Протоколы уровня представления: AFP — Apple Filing Protocol, ICA — Independent Computing Architecture, LPP — Lightweight Presentation Protocol, NCP — NetWare Core Protocol, NDR — Network Data Representation, RDP — Remote Desktop Protocol, XDR — eXternal Data Representation, X.25 PAD — Packet Assembler/Disassembler Protocol.

- **Сеансовый уровень (5)**

Сеансовый уровень (англ. session layer) модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Протоколы сеансового уровня: ADSP (AppleTalk Data Stream Protocol), ASP (AppleTalk Session Protocol), H.245 (Call Control Protocol for Multimedia Communication), ISO-SP (OSI Session Layer Protocol (X.225, ISO 8327)), iSNS (Internet Storage Name Service), L2F (Layer 2 Forwarding Protocol), L2TP (Layer 2 Tunneling Protocol), NetBIOS (Network Basic Input Output System), PAP (Password Authentication Protocol), PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call Protocol), RTCP (Real-time Transport Control Protocol), SMPP (Short Message Peer-to-Peer), SCP (Secure Copy Protocol), ZIP (Zone Information Protocol), SDP (Sockets Direct Protocol).

- **Транспортный уровень (4)**

Транспортный уровень (англ. transport layer) модели OSI предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом собственно надёжность может варьироваться в широких пределах.

Основной протокол транспортного уровня - **TCP (Transmission Control Protocol)** – описывает, каким образом на стороне отправителя передаваемая информация нарезается на стандартные пакеты, которые маркируются, а затем – как на стороне получателя полученные пакеты собираются в единый объект.

Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных.

Например, UDP ограничивается контролем целостности данных в рамках одной датаграммы и не исключает возможности потери пакета целиком либо дублирования пакетов или нарушения порядка получения пакетов данных А протокол TCP, например, обеспечивает надёжную непрерывную передачу данных, исключающую потерю данных или нарушение порядка их поступления либо дублирования, и может перераспределять данные, разбивая большие порции данных на фрагменты и, наоборот, склеивая фрагменты в один пакет.

Протоколы транспортного уровня: ATP (AppleTalk Transaction Protocol), CUDP (Cyclic UDP), DCCP (Datagram Congestion Control Protocol), FCP (Fiber Channel Protocol), IL (IL Protocol), NBF (NetBIOS Frames protocol), NCP (NetWare Core Protocol), SCTP (Stream Control Transmission Protocol), SPX (Sequenced Packet Exchange), SST (Structured Stream Transport), TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

- **Сетевой уровень (3)**

Сетевой уровень (network layer) предназначен для определения пути передачи данных. Он отвечает за трансляцию логических адресов и имён в физические и определение кратчайших маршрутов, а также – за коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.

Основной протокол сетевого уровня- **IP (Internet Protocol)** - описывает, каким образом конструируются и присваиваются адреса тем или иным сетевым (информационно-техническим) объектам.

Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего

Протоколы сетевого уровня: IP/IPv4/IPv6 (Internet Protocol), IPX (Internetwork Packet Exchange, протокол межсетевого обмена), X.25 (частично этот протокол реализован на уровне 2), CLNP (сетевой протокол без организации соединений), IPsec (Internet Protocol Security), ICMP (Internet Control Message Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First), ARP (Address Resolution Protocol).

- **Канальный уровень (2)**

Канальный уровень (англ. data link layer – dll) предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля за ошибками, которые могут возникнуть. Этот уровень упаковывает в кадры полученные с физического уровня данные, проверяет их на целостность, а если нужно – исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет информацию на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Спецификация IEEE 802 разделяет этот уровень на два подуровня:

MAC (англ. media access control) регулирует доступ к разделяемой физической среде;

LLC (англ. logical link control) обеспечивает обслуживание сетевого уровня.

На этом уровне работают коммутаторы, мосты и другие устройства. В программировании этот уровень представляет драйвер сетевой платы, а в операционных системах имеется программный интерфейс взаимодействия канального и сетевого уровней между собой. Но это не новый уровень, а просто реализация модели для конкретной ОС. Примеры таких интерфейсов: ODI, NDIS, UDI.

Протоколы канального уровня: ARCnet, ATM, Cisco Discovery Protocol (CDP), Controller Area Network (CAN), Econet, Ethernet, Ethernet Automatic Protection Switching (EAPS), Fiber Distributed Data Interface (FDDI), Frame Relay, High-Level Data Link Control (HDLC), IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers), Link Access Procedures, D channel (LAPD), IEEE 802.11 wireless LAN, LocalTalk, Multiprotocol Label Switching (MPLS), Point-to-Point Protocol (PPP), Point-to-Point Protocol over Ethernet (PPPoE), Serial Line Internet Protocol (SLIP, obsolete), StarLan, Spanning tree protocol, Token ring, Unidirectional Link Detection (UDLD), x.25.

- **Физический уровень (1)**

Физический уровень (англ. physical layer) — нижний уровень модели, предназначенный непосредственно для передачи потока данных. Этот уровень осуществляет передачу электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их приём и преобразование в биты данных в соответствии с методами кодирования цифровых сигналов. Другими словами, уровень 1 осуществляет интерфейс между сетевым носителем и сетевым устройством.

На этом уровне работают концентраторы, повторители сигнала и медиаконвертеры. Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие виды среды передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п.

Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются: V.35, RS-232, RS-485, RJ-11, RJ-45, а также разъемы AUI и BNC.

Протоколы физического уровня: IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11 Wi-Fi, Etherloop, GSM Um radio interface, ITU и ITU-T, TransferJet, ARINC 818, G.hn/G.9960.

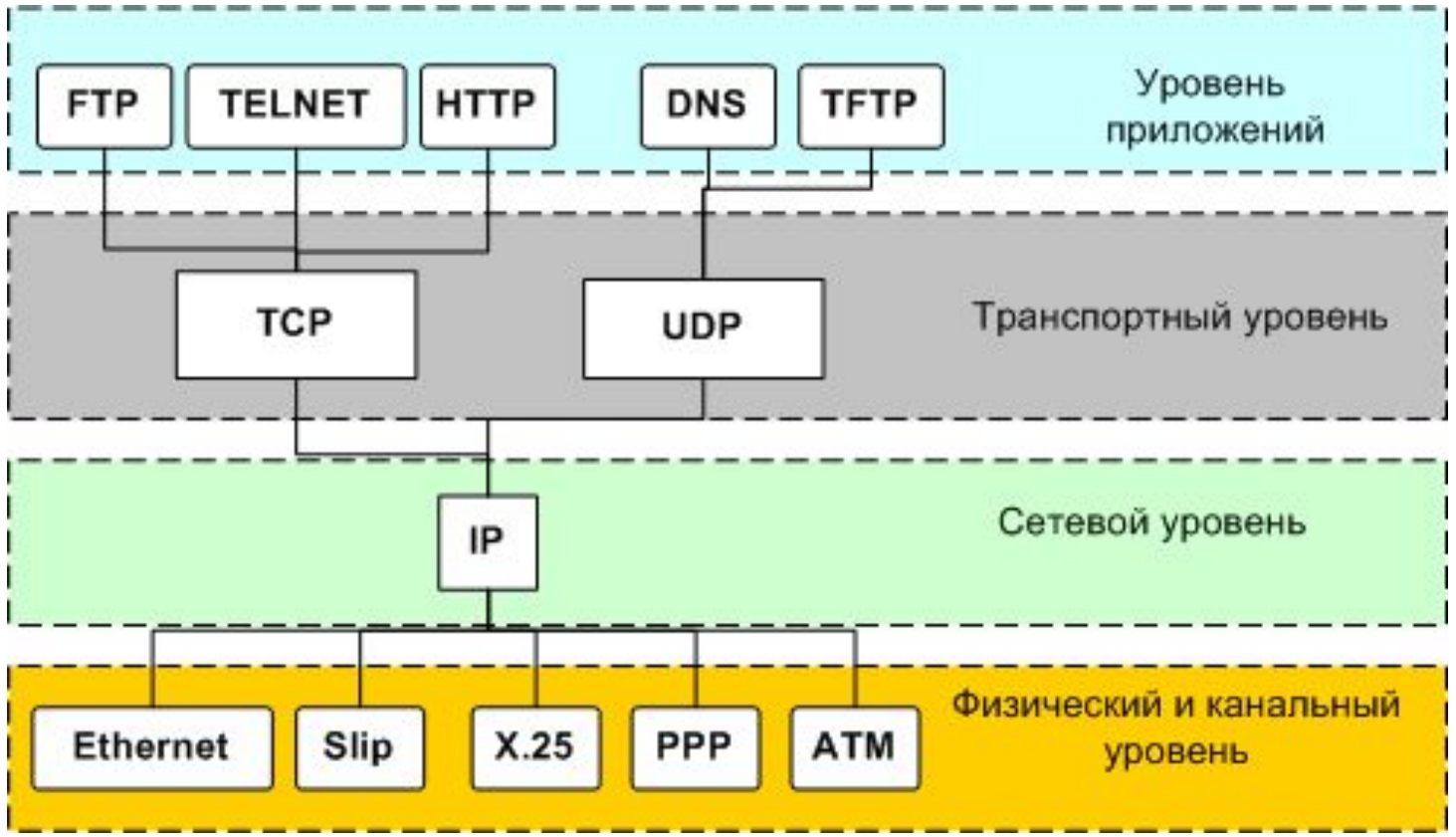
- **Соответствие модели OSI других моделей сетевого взаимодействия**

Множество протоколов, наиболее востребованных и практически используемых, было разработано с использованием других моделей (не OSI) сетевого взаимодействия. Например, основной, используемый в настоящее время, стек протоколов — TCP/IP – возник ещё до принятия модели OSI и вне связи с ней.

В этом контексте важным является вопрос возможного включения отдельных протоколов других моделей в различные уровни модели OSI.

- **Семейство TCP/IP** имеет два транспортных протокола:
  - TCP, полностью соответствующий OSI, обеспечивающий проверку получения данных;
  - UDP, отвечающий транспортному уровню только наличием порта, обеспечивающий обмен датаграммами между приложениями, не гарантирующий получения данных.

В целом же в семействе TCP/IP есть ещё около 200 протоколов, многие из которых не являются строго транспортными протоколами. Самым известным из этого семейства является служебный протокол ICMP, используемый для обеспечения определенных внутренних нужд взаимодействия.



- **Семейство IPX/SPX**

В семействе IPX/SPX порты (называемые сокетами или гнёздами) появляются в протоколе сетевого уровня IPX, обеспечивая обмен датаграммами между приложениями (операционная система резервирует часть сокетов для себя). Протокол SPX, в свою очередь, дополняет IPX всеми остальными возможностями транспортного уровня в полном соответствии с OSI.

В качестве адреса хоста IPX использует идентификатор, образованный из четырёхбайтного номера сети (назначаемого маршрутизаторами) и MAC-адреса сетевого адаптера.

- **Критика модели OSI**

В конце 90-х годов семиуровневая модель OSI яростно критиковалась отдельными авторами. В частности, в книге «UNIX. Руководство системного администратора» Эви Немет (англ. Evi Nemeth) писала: «Пока комитеты ISO спорили о своих стандартах, за их спиной менялась вся концепция организации сетей и по всему миру внедрялся протокол TCP/IP».

И вот, когда протоколы ISO были наконец реализованы, отмечала она, выявился целый ряд проблем:

- эти протоколы основывались на концепциях, не имеющих в современных сетях никакого смысла (бурное развитие сетей «обогнало» концепции);
- их спецификации были в некоторых случаях неполными;
- по своим функциональным возможностям они уступали другим современным протоколам;
- наличие многочисленных уровней сделало эти протоколы медлительными и трудными для реализации.

Эви Немет заявляла также: «сейчас даже самые рьяные сторонники этих протоколов признают, что OSI постепенно движется к тому, чтобы стать маленькой сноской на страницах истории компьютеров».

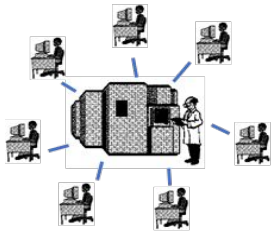
Однако это предсказание, как видим, все еще не сбылось.

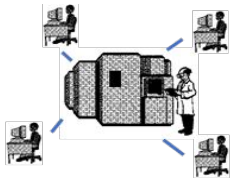
История возникновения сети Интернет

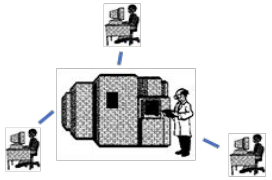
- В 1969 году Министерство Обороны США создало сеть, которая явилась предтечей Internet, – она называлась ARPAnet и была экспериментальной сетью, поскольку создавалась для поддержки научных исследований в военно-промышленной сфере, в частности, для исследования методов построения сетей, устойчивых к частичным повреждениям, получаемым при бомбардировке авиацией, и способных в таких условиях продолжать нормальное функционирование.
- В модели ARPAnet всегда была связь между компьютером-источником и компьютером-приемником (станцией назначения). Сеть предполагалась ненадежной: любая часть сети может исчезнуть в любой момент.
- На связывающиеся компьютеры – не только на саму сеть – также возложена ответственность, обеспечивать налаживание и поддержание связи. Основной принцип состоял в том, что любой компьютер мог связаться как равный с равным с любым другим компьютером.
- Передача данных в сети была организована на основе протокола Internet – IP, который включает правила налаживания и поддержания связи в сети, правила обращения с IP-пакетами и их обработки, описания сетевых пакетов семейства IP (их структура и т. п.). Сеть задумывалась и проектировалась так, чтобы от пользователей не требовалось знаний о структуре сети.
- Для того, чтобы послать сообщение по сети, компьютер должен поместить данные в некий "конверт", указать на нем конкретный адрес в сети и передать получившиеся пакеты в сеть.

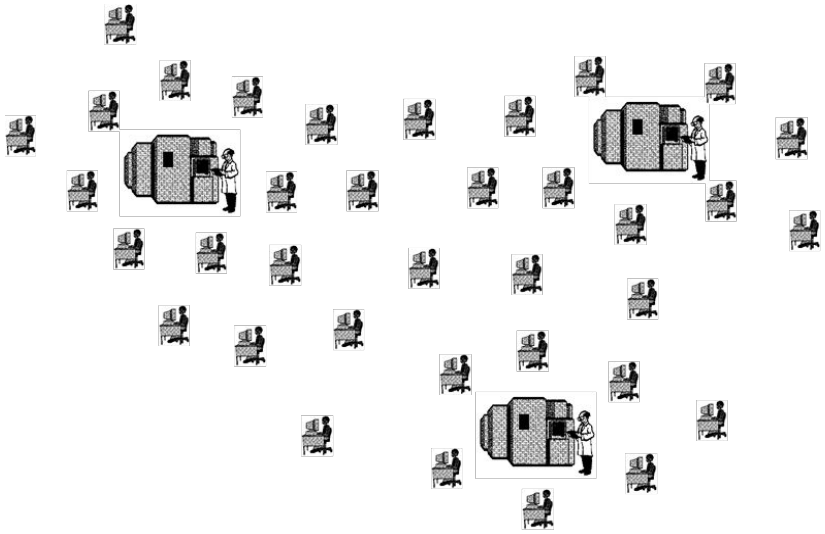
- Пока Международная Организация по Стандартизации (Organization for International Standardization – ISO) тратила годы, создавая окончательный стандарт для компьютерных сетей, пользователи ждать не желали. Активисты Internet начали устанавливать IP-программное обеспечение на все возможные типы компьютеров.
- Вскоре это стало единственным приемлемым способом для связи разнородных компьютеров. Такая схема понравилась правительству и университетам, которые проводили политику покупки компьютеров у различных производителей.
- Примерно 10 лет спустя после появления ARPAnet появились Локальные Вычислительные Сети (LAN), например, такие как Ethernet и др. Одновременно появились компьютеры, которые стали называть рабочими станциями. На большинстве рабочих станций была установлена операционная система UNIX. Эта ОС имела возможность работы в сети с протоколом Internet (IP). В связи с возникновением принципиально новых задач и методов их решения появилась новая потребность: организации желали подключиться к ARPAnet своей локальной сетью. Примерно в то же время появились другие организации, которые начали создавать свои собственные сети, использующие близкие к IP коммуникационные протоколы.
- Стало ясно, что все только выиграли бы, если бы эти сети могли общаться все вместе, ведь тогда пользователи из одной сети смогли бы связываться с пользователями другой сети.

- Одной из важнейших среди этих новых сетей была NSFnet, разработанная по инициативе Национального Научного Фонда (National Science Foundation – NSF). В конце 80-х годов NSF создал пять суперкомпьютерных центров, сделав их доступными для использования в любых научных учреждениях. Было создано всего лишь пять центров потому, что они очень дороги даже для богатой Америки. Именно поэтому их и следовало использовать кооперативно. Возникла проблема связи: требовался способ соединить эти центры и предоставить доступ к ним различным пользователям. Сначала была сделана попытка использовать коммуникации ARPAnet, но это решение потерпело крах, столкнувшись с бюрократией оборонной отрасли и проблемой обеспечения персоналом.
- Тогда NSF решил построить свою собственную сеть, основанную на IP технологии ARPAnet. Центры были соединены специальными телефонными линиями с пропускной способностью 56 KBPS (7 KB/s). Однако, было очевидно, что не стоит даже и пытаться соединить все университеты и исследовательские организации непосредственно с центрами, т. к. проложить такое количество кабеля – не только очень дорого, но практически невозможно.
- Поэтому решено было создавать сети по региональному принципу. В каждой части страны заинтересованные учреждения должны были соединиться со своими ближайшими соседями.
- Получившиеся цепочки подсоединялись к суперкомпьютеру в одной из своих точек, таким образом суперкомпьютерные центры были соединены вместе.
- В такой топологии любой компьютер мог связаться с любым другим, передавая сообщения через соседей.









- Это решение было успешным, но настала пора, когда сеть уже более не справлялась с возросшими потребностями. Совместное использование суперкомпьютеров позволяло подключенным общинам использовать и множество других вещей, не относящихся к суперкомпьютерам.
- Неожиданно университеты, школы и другие организации осознали, что заимели под рукой море данных и мир пользователей. Поток сообщений в сети (трафик) нарастал все быстрее и быстрее пока, в конце концов, не перегрузил управляющие сетью компьютеры и связывающие их телефонные линии.
- В 1987 г. контракт на управление и развитие сети был передан компании Merit Network Inc., которая занималась образовательной сетью Мичигана совместно с IBM и MCI. Старая физически сеть была заменена более быстрыми (примерно в 20 раз) телефонными линиями. Были заменены на более быстрые и сетевые управляющие машины.
- Процесс совершенствования сети идет непрерывно. Однако, большинство этих перестроек происходит незаметно для пользователей. Включив компьютер, вы не увидите объявления о том, что ближайшие полгода Internet не будет доступна из-за

Глобальные компьютерные сети

- Глобальными называются сети, охватывающие большие территории и включающая в себя большое число компьютеров, рассредоточенных на расстоянии сотен и тысяч километров. Для обозначения таких сетей используются аббревиатуры ГВС, ГКС, WAN (Wide Area Network).
- В отличие от локальных сетей (LAN) глобальные сети не имеют границ.
- ГВС служат для объединения разрозненных сетей так, чтобы пользователи и компьютеры, где бы они ни находились, могли взаимодействовать со всеми остальными участниками глобальной сети.
- Некоторые ГВС построены исключительно для частных организаций, другие являются средством коммуникации корпоративных ЛВС (локальных сетей) с сетью Интернет или посредством Интернет - с удалёнными сетями, входящими в состав корпоративных. Чаще всего ГВС опирается на выделенные линии, на одном конце которых маршрутизатор подключается к ЛВС, а на другом концентратор связывается с остальными частями ГВС. Основными используемыми протоколами являются: TCP/IP, SONET/SDH, MPLS, ATM и FR.
- Наиболее известными ГВС являются:

  Интернет (Internet);

  Фидонет (FidoNet).

- **Фидонет (FidoNet)** — международная любительская компьютерная сеть, построенная по технологии «из точки в точку». Изначально программное обеспечение FidoNet разрабатывалось под MS-DOS, однако в скором времени было портировано под все распространённые операционные системы, включая UNIX, Linux, Windows, OS/2 и Mac.

- Сеть была создана в 1984 год американским программистом Томом Дженнингсом. Передача сообщений в этой сети осуществлялась в ночные часы, когда стоимость телефонных звонков была ниже. Для обмена почтой с другим узлом сети был выделен один час, в течение которого доступ сторонних пользователей был закрыт. Этот час позже получил название «национального почтового часа».
- В России первый узел сети был создан в 1990 году в Новосибирске.
- Фидонет достигла пика своей популярности в 1996 году, когда численность состоящих в ней узлов составляла почти 40 000. Однако и до настоящего времени эта сеть остается достаточно популярной: в 2010 году в ней насчитывалось более 5 000 узлов.
- В 2000-х годах произошел мощный отток пользователей из сети Фидонет в блоги и социальные сети Интернета. Однако активность Фидонета сохраняется и сегодня. Например, в соответствии со статистикой только за октябрь 2015 года на узле 5030/722 прошло нескольких тысячах сообщений в популярных эхоконференциях.
- Общение пользователей сети Фидонет происходит двумя способами: а) личная переписка (нетмейл, Netmail); б) эхоконференции (эхи) – коллективные обсуждения. Жаргонное название пользователей сети Фидонет — фидошники. Шутливая расшифровка аббревиатуры ФИДО - Федерация исключительно дружеского общения.
- На базе ПО сети Фидонет были созданы и другие сети, получившие общее название — FTN (англ. Fidonet technology network). В народе такие сети ещё называют «левонеты».
- В 1990-е годы ряд банков применяли FTN-технологию для связи с филиалами и создания систем «Клиент-банк». А некоторые предприятия и по сей день используют FTN-сети в качестве транспорта для обмена информацией, если организация иного канала невозможна или нецелесообразна по каким-либо причинам.

- Особенностью FidoNet, определившей широкое распространение этой сети в России, является фактическая бесплатность подключения и использования ресурсов сети
- Фидонет является офлайновой сетью, то есть сообщения и файлы хранятся на компьютере пользователя, а обрабатываются и подготавливаются к отправке в то время, когда пользователь может быть отключен от сети. Таким образом, для работы с сетью не требуется постоянное подключение к ней.
- Сеть Фидонет не является частью сети Интернет, однако, сегодня каналы и протоколы Интернета часто используются для передачи трафика Фидонет. Кроме того, большая часть эхоконференций сети Фидонет доступна пользователям сети Интернет через сеть Usenet и WWW-гейты / WebBBS / фидофорумы – специальные WWW-сайты, предоставляющий доступ к эхоконференциям сети Фидонет. Технически – это шлюзы (гейты) между сетью WWW и сетью Фидонет, преобразующие форму информации из протокола binkp (технология FTN) в протокол HTTP (технология WWW) и обратно.
- Днем рождения **Интернет** в современном понимании этого слова стала дата стандартизации протокола связи TCP/IP, лежащего в основе Всемирной сети по нынешний день. На самом деле TCP/IP - это стек протоколов, то есть два неразрывно связанных протокола, лежащих на разных уровнях сетевого взаимодействия.
- **TCP** (Transmission Control Protocol) — протокол транспортного уровня, управляющий передачей информации. Согласно этому протоколу отправляемые данные «нарезаются» на небольшие, строго стандартные пакеты, после чего каждый пакет маркируется таким образом, чтобы эти специальные метки позволяли правильно «собрать» документ на компьютере получателя.
- **IP** (Internet Protocol) — адресный протокол. Он принадлежит сетевому уровню и определяет, куда происходит передача. Его суть состоит в том, что у каждого участника Всемирной сети (т. е. компьютера, подключенного к сети) должен быть свой уникальный адрес: IP - адрес, имеющий специальную цифровую форму. Адрес состоит из четырех чисел, разделенных точкой. Каждое число может принимать 256 различных значений в интервале от 0 до 255 включительно. Вид такого адреса может быть, например, таким: 195.38.46.11.

Доменная структура сети

- Когда компьютеры объединяются в сеть, они группируются в рабочие группы или домены. Компьютеры, входящие в один домен, могут располагаться в локальной сети, в разных странах и на континентах. Структура указанных связей компьютеров в сети отражается в их сетевых именах, присваиваемых в соответствии с международным стандартом.

IP-адресация (*Internet Protocol Address*)

- IP-адрес — это уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. В сети Интернет требуется глобальная уникальность адреса в отличие от локальной сети, где требуется уникальность адреса только в пределах ЛВС. По функции сетевые адреса аналогичны традиционным почтовым адресам: по ним доставляется информация от отправителя к адресату.
- В версии протокола IPv4 IP-адрес имеет длину 4 байта, в IPv6 — 16 байт. Адрес состоит из двух частей:
  - одна характеризует адрес сети,
  - другая - адрес компьютера в данной сети.
- В 4-й версии IP-адрес представляет собой 32-битовое число. Маска записи: четыре десятичных числа значением от 0 до 255, разделённых точками, например, 172.168.0.16 или 192.0.2.60.
- В 6-й версии IP-адрес (IPv6) является 128-битовым. Внутри адреса разделителем является двоеточие (напр. 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Ведущие нули допускается в записи опускать. Нулевые группы, идущие подряд, могут быть также опущены, вместо них ставится двойное двоеточие (2001:0db8:0:0:0:0:0:1 можно записать как 2001:0db8::::::1). Более одного такого пропуска в адресе не допускается.

<u>Статические и динамические IP-адреса</u>

- IP-адрес называют ***статическим*** (*постоянным*, *неизменяемым*) в двух случаях:
  - когда адрес задан пользователем в настройках устройства;
  - когда адрес записан в конфигурации сервера (службы) распределения адресов (DHCP, BOOTP и др.) и поэтому выдаётся устройству в качестве постоянного.

Преимущества статического адреса IP:

- возможность сделать постоянную запись доменного имени в DNS, как прямую, так и обратную;
- простота организации сервера любой интернет-службы, например, веб-сервера или сервера

- IP-адрес называют ***динамическим*** (*непостоянным*, *изменяемым*), если он назначается при подключении устройства к сети автоматически из некоторого диапазона и используется в течение ограниченного промежутка времени. (Диапазон и время жизни указываются в конфигурации службы назначения адресов IP).
- Динамическая выдача адресов используется провайдерами в целях экономии адресов IPv4 и в локальных сетях для удобства администрирования.

Недостатки динамического адреса:

- невозможность работы на динамическом хосте для некоторых служб (DNS, IPSEC, …).
- сложность поддержания записи доменного имени хоста в системе DNS.
- практически невозможно сделать запись в обратной зоне DNS.
- невозможность реальной работы почтового сервера на динамическом адресе: диапазоны динамических адресов, как правило, оказываются в списках блокировки.
- невозможно обеспечить непрерывную доступность интернет-сервисов на динамическом хосте, т. к. при изменении адреса IP требуется некоторое время нужно для того, чтобы информация об этом изменении разошлась по серверам имён и "ушла" из кешей систем и серверов.

Протоколы для получения клиентом адреса IP:

- DHCP (RFC 2131) — наиболее распространённый протокол настройки сетевых параметров;
- BOOTP (RFC 951) — простой протокол настройки сетевого адреса, обычно используется для бездисковых станций;
- IPCP (RFC 1332) — распространённый протокол настройки сетевых параметров в соединениях PPP (RFC 1661);
- Zeroconf (RFC 3927) — протокол настройки сетевого адреса, определения имени, поиск служб.

DNS-адресация

- Цифровая запись слишком сложна для того, чтобы человек мог запомнить хотя бы несколько адресов. Поэтому была создана система, позволяющая назначать компьютерам именные (текстовые) адреса и соотносить их с цифровыми.
- DNS (Domain Name Service) – распределенная система баз данных для перевода текстовых компьютерных имен в цифровые адреса Internet. Процессом оформления и поддержания доменных имен занимается ряд специализированных организации. Именные адреса имеют не все компьютеры, как правило, именные адреса используют компьютеры-серверы (хост-компьютеры), организующие доступ к различным услугам. Выделяют три вида адресов:

1) адрес компьютера-сервера (хост-компьютера)

ДоменТретьегоУровня.**ДоменВторогоУровня.ДоменПервогоУровня (зона)**

lady.mail.ru

2) адрес электронной почты

Пользователь@ДоменВторогоУровня.ДоменПервогоУровня(зона)

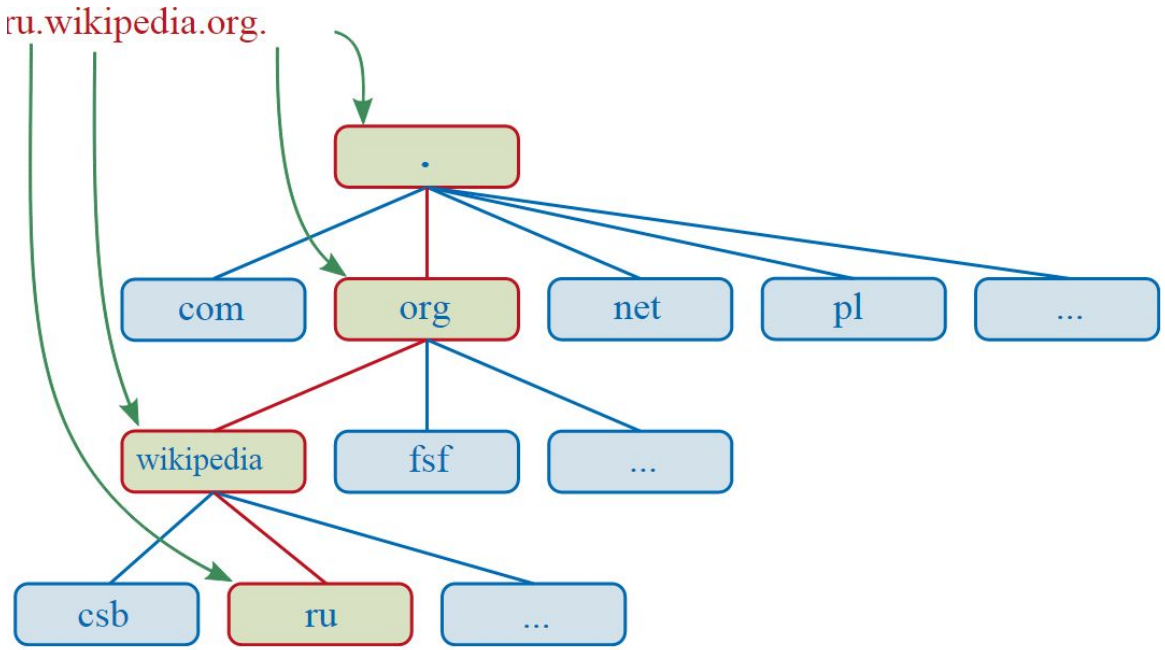
mamoyklanus@yandex.com

По состоянию на июль 2011 года:

- самые крупные доменные зоны (по убыванию): COM, DE, NET, UK, ORG, CN, INFO, NL, RU, EU;

Имя	.com	.net	.org	.info	.biz	.ru	.рф	.su
Кол-во	95 871 283	14 004 705	9 266 204	7 914 762	2 106 138	3 337 940	858 734	93 883

- общая численность доменов 2-го уровня во всех доменах 1-го уровня превысила 225 млн имен.



Соотношение доменного имени и IP-адреса

Доменное имя и IP-адрес не тождественны:

- один IP-адрес может иметь множество имён, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется виртуальный хостинг). Наличие многих тысяч доменных имён с разными сайтами может вызывать проблемы при идентификации сайтов по IP-адресу, например, в целях цензуры;
- одно доменное имя может соответствовать нескольким IP-адресам (например, для распределения нагрузки по нескольким ЭВМ).
- один сервер с одним доменным именем может содержать несколько разных сайтов, а части одного сайта могут быть доступны по разным доменным именам (например, для изоляции cookies и скриптов в целях защиты от атак типа межсайтового скриптинга).

- **URL-адресация**
- Не всегда нам важно знать цифровой или текстовый адрес (имя) компьютера. Нередко нам требуется лишь адрес конкретного файла.
- Адрес любого файла во всемирном масштабе определяется унифицированным указателем ресурса – URL (*Uniform Resource Locator)*. единообразный локатор (определитель местонахождения) ресурса. URL служит стандартизированным способом записи адреса ресурса в сети Интернет.

Адрес URL состоит из трех частей:

- указание службы, которая осуществляет доступ к данному ресурсу. Обычно обозначается именем прикладного протокола, соответствующего данной службе (http://…);
- указание доменного имени компьютера-сервера на котором хранится данный ресурс (http://abcde.com);
- указания полного пути доступа к файлу на данном компьютере.

Например:

http://www.for-stydents.ru/tulgu/informatika/lekcii-po-informatike-1-kurs.html

Здесь http - схема обращения к ресурсу (в большинстве случаев имеется в виду сетевой протокол). Общепринятые схемы (протоколы) URL включают:

ftp — Протокол передачи файлов FTP
http — Протокол передачи гипертекста HTTP
https — Специальная реализация протокола HTTP, использующая шифрование (как правило, SSL или TLS)
mailto — Адрес электронной почты
news — Новости Usenet
nntp — Новости Usenet через протокол NNTP
telnet — Ссылка на интерактивную сессию Telnet
file — Имя локального файла
data — Непосредственные данные (Data: URL)
tel — Звонок по указанному телефону
skype — Протокол Skype
smsto — Открытие редактора SMS в некоторых мобильных телефонах

Однако стандарт URL обладает серьёзным недостатком — в нём можно использовать только ограниченный набор символов: латинские буквы, цифры и лишь некоторые знаки препинания. Если мы захотим использовать в URL символы кириллицы или иероглифы, а также некоторые французского языка, то они должны быть перекодированы особым образом.

Например, слово «Микрокредит» кодируется в URL как:
%D0%9C%D0%B8%D0%BA%D1%80%D0%BE%D0%BA%D1%80%D0%B5%D0%B4%D0%B8%D1%82

Протоколы и сервисы Интернет

Сетевые протоколы

Протоколы прикладного уровня используются в конкретных прикладных программах. Общее их количество велико и продолжает постоянно увеличиваться. Некоторые приложения существуют с самого начала развития Internet, например, TELNET и FTP. Другие появились позже: HTTP, NNTP, POP3, SMTP.

- Протокол TELNET - позволяет серверу рассматривать все удаленные компьютеры как стандартные «сетевые терминалы» текстового типа. Работа с TELNET походит на набор телефонного номера. Пользователь набирает на клавиатуре что-то вроде telnet delta и получает на экране приглашение на вход в машину delta. Протокол TELNET существует уже давно. Он хорошо опробован и широко распространен. Создано множество реализаций для самых разных операционных систем.

- Протокол FTP - (File Transfer Protocol – протокол передачи файлов) распространен так же широко, как TELNET. Он является одним из старейших протоколов семейства TCP/IP. Также как TELNET он пользуется транспортными услугами TCP. Существует множество реализаций для различных операционных систем, которые хорошо взаимодействуют между собой. Пользователь FTP может вызывать несколько команд, которые позволяют ему посмотреть каталог удаленной машины, перейти из одного каталога в другой, а также скопировать один или несколько файлов.

- Протокол SMTP - (Simple Mail Transfer Protocol – простой протокол передачи почты) поддерживает передачу сообщений (электронной почты) между произвольными узлами сети internet. Имея механизмы промежуточного хранения почты и механизмы повышения надежности доставки, протокол SMTP допускает использование различных транспортных служб.

Протокол SMTP обеспечивает как группирование сообщений в адрес одного получателя, так и размножение нескольких копий сообщения для передачи в разные адреса. Над модулем SMTP располагается почтовая служба конкретного компьютера. В типичных программах-клиентах в основном применяется для отправки исходящих сообщений.

- Протокол HTTP - (Hypertext transfer protocol – протокол передачи гипертекста) применяется для обмена информацией между серверами WWW (World Wide Web – всемирная паутина) и программами просмотра гипертекстовых страниц – браузерами WWW. Допускает передачу широкого спектра разнообразной информации – текстовой, графической, аудио и видео. В настоящее время находится в стадии непрерывного совершенствования.

- Протокол POP3 - (Post Office Protocol – протокол почтового узла, 3 версия) позволяет программам-клиентам электронной почты принимать и передавать сообщения с/на почтовые серверы. Обладает достаточно гибкими возможностями по управлению содержимым почтовых ящиков, расположенных на почтовом узле. В типичных программах-клиентах в основном применяется для приема входящих сообщений.

- Протокол NNTP - (Network News Transfer Protocol – протокол передачи сетевых новостей) позволяет общаться серверам новостей и клиентским программам – распространять, запрашивать, извлекать и передавать сообщения в группы новостей. Новые сообщения хранятся в централизованной базе данных, которая позволяет пользователю выбирать интересующие его сообщения. Также обеспечивается индексирование, организация ссылок и удаление устаревших сообщений.

Сетевые сервисы

В простейшем понимании сетевой сервис (услуга, служба) - это две программы, взаимодействующие между собой согласно определенным правилам, называемым протоколами. Одна программа называется сервером (предоставляет услуги), вторая называется клиентом (принимает услуги).

Таким образом, если речь идет о работе служб Интернет, то между собой взаимодействуют:

- оборудование-сервер и оборудование-клиент;
- программа-сервер и программа-клиент.

Разные службы имеют разные протоколы, которые называются прикладными протоколами.

Каждый вид сервиса в Internet предоставляется соответствующими серверами и может использоваться с помощью соответствующих клиентов. Серверами называются узлы сети, предназначенные для обслуживания запросов клиентов – программных агентов, извлекающих информацию или передающих ее в сеть и работающих под непосредственным управлением пользователей. Клиенты предоставляют информацию в понятном и удобном для пользователей виде, в то время как серверы выполняют служебные функции по хранению, распространению, управлению информацией и выдачу ее по запросу клиентов.

Сервис WWW – (World Wide Web - всемирная паутина) обеспечивает представление и взаимосвязи огромного количества гипертекстовых документов, включающих текст, графику, звук и видео, расположенных на различных серверах по всему миру и связанных между собой посредством ссылок (гиперссылок) в документах. Таким образом, WWW — это единое информационное пространство, состоящее из огромного количества взаимосвязанных Web — страниц.

- Группы тематически оформленных Web- страниц называют Web - узлами или Web - сайтами. Один физический Web - сервер может содержать достаточно много Web - узлов. Появление этого сервиса значительно упростило доступ к информации и стало одной из основных

- Большая часть документов в системе WWW хранится в формате HTML (сетевым сервисом не является). HTML (HyperText Markup Language) - это язык гипертекстовой разметки, используемой для кодирования информации. Язык HTML представляет собой набор команд, в соответствии с которыми браузер отображает содержимое документа, при этом сами команды HTML не отображаются. В языке HTML реализован механизм гипертекстовых ссылок, который обеспечивает связь одного документа с другими (гиперссылка обычно выделена подчеркиванием или жирным шрифтом). Команды в тексте HTML-документа называются тегами. Тег HTML может содержать список атрибутов. Теги заключены в угловые скобки. Большинство тегов используются парами. Например, тег <CENTER>text</CENTER> применяется для выравнивания текста по центру.
- Почти все, что сопровождает деятельность современного человека, ассоциируется с понятием «работа в системе Internet»: от самых последних финансовых новостей до информации о медицине и здравоохранении, музыке и литературе, домашних животных и комнатных растениях, кулинарии и автомобильном деле. Можно заказывать авиабилеты в любую часть мира (реальные, а не виртуальные), туристические проспекты, находить необходимое программное и техническое обеспечение для своего ПК, играть в игры с далекими (и неизвестными) партнерами и следить за спортивными и политическими событиями в мире. Наконец, с помощью большинства программ со средствами доступа к WWW можно получить доступ и к телеконференциям (всего их около 10 000), куда помещаются сообщения на любые темы – от астрологии до языкознания, а также обмениваться сообщениями по электронной почте.
- Благодаря средствам просмотра WWW хаотические джунгли информации в Internet приобретают форму привычных аккуратно оформленных страниц с текстом и фотографиями, а в некоторых случаях даже с видеосюжетами и звуком. Привлекательные титульные страницы (home pages) сразу же помогают понять, какая информация последует дальше. Здесь есть все необходимые заголовки и подзаголовки, выбирать которые можно с помощью линеек прокрутки как на обычном экране Windows или Macintosh. Каждое ключевое слово соединяется с соответствующими информационными файлами посредством гипертекстовых связей.

Сервис E-MAIL - электронная почта, с помощью которой можно обмениваться личными или деловыми сообщениями между адресатами, имеющими электронный адрес.

- Услуги электронной почты предоставляются провайдерами, которые выделяют клиентам место на своем сервере для корреспонденции, поддерживают системы идентификации, учета пользователей и их прав, а также предоставляют сопутствующие услуги
- Для передачи сообщений в основном используется протокол SMTP, а для приема – POP3.

Сервис NEWS/USENET – это всемирный дискуссионный клуб. Он состоит из набора конференций («newsgroups»), имена которых организованы иерархически в соответствии с обсуждаемыми темами. Сообщения («articles» или «messages») посылаются в эти конференции пользователями посредством специального программного обеспечения. Приходящие от пользователя сообщения рассылаются на серверы новостей и становятся доступными для прочтения другими пользователями.

- Можно послать сообщение и просмотреть отклики на него, которые появятся в дальнейшем. Так как один и тот же материал читает множество людей, то отзывы начинают накапливаться. Все сообщения по одной тематике образуют поток («thread») [в русском языке в этом же значении используется и слово «тема»]; таким образом, хотя отклики могли быть написаны в разное время и смешаться с другими сообщениями, они все равно формируют целостное обсуждение.
- Вы можете подписаться на любую конференцию, просматривать заголовки сообщений в ней с помощью программы чтения новостей, сортировать сообщения по темам, чтобы было удобнее следить за обсуждением, добавлять свои сообщения с комментариями и задавать вопросы. Для прочтения и отправки сообщений используются программы чтения новостей, например, Netscape News, встроенная в браузер Netscape Navigator, а также программа Internet News от Microsoft, поставляемая вместе с последними версиями Internet Explorer.

Сервис FTP – это метод пересылки файлов между компьютерами. Продолжающиеся разработка программного обеспечения и публикация уникальных текстовых источников информации гарантируют постоянный интерес пользователей к мировым архивам FTP, постоянно меняющейся сокровищницей.

- FTP-архивы содержат как общедоступные бесплатные программы (publicdomain, так и условно-бесплатное программное обеспечение (shareware), т.к. потребуется заплатить автору, если по окончании срока пробной эксплуатации вы решите оставить себе программу. Имеются и т.н. бесплатные программы (freeware) – их создатели сохраняют за собой авторские права, но никакой платы за пользование

- Для просмотра FTP-архивов и получения хранящихся на них файлов можно воспользоваться специализированными программами – WS_FTP, CuteFTP, или же использовать браузеры, в которых содержатся встроенные средства работы с FTP-серверами, например, Netscape Navigator, Internet Explorer т др.

Сервис TELNET – это возможность работы на удаленном компьютере в режиме (удаленного доступа), когда ваш компьютер эмулирует терминал удаленного компьютера. Таким образом, вы можете делать все то же (или почти то же), что можно делать с обычного терминала машины, с которой вы установили сеанс удаленного доступа.

- Программа, которая обслуживает удаленные сеансы, называется telnet. Этот сервис имеет набор команд, которые управляют сеансом связи и его параметрами. Сеанс обеспечивается совместной работой программного обеспечения удаленного компьютера и вашего. Они устанавливают TCP-связь и общаются через TCP и UDP пакеты.
- Программа telnet входит в поставку Windows и устанавливается вместе с поддержкой протокола TCP/IP.

Сервис PROXY-сервер - («ближний» сервер) предназначен для накопления информации, к которой часто обращаются пользователи, в локальной системе. При подключении к Internet с использованием proxy-сервера запросы первоначально направляются на эту локальную систему. Сервер извлекает требуемые ресурсы и предоставляет их вам, одновременно сохраняя копию. При повторном обращении к тому же ресурсу предоставляется сохраненная копия. Таким образом, уменьшается количество удаленных соединений.

- Использование proxy-сервера может несколько увеличить скорость доступа, если канал связи вашего провайдера Internet недостаточно производителен. Если же канал связи достаточно мощный, скорость доступа может даже несколько снизиться, поскольку при извлечении ресурса вместо одного соединения от пользователя к удаленному компьютеру производится два: от пользователя к proxy-серверу и от proxy-сервера к удаленному компьютеру.

На основе перечисленных и многих других (которые постоянно множатся) протоколов и сервисов Интернет функционируют многочисленные другие известные и не очень сервисы и возможности: списки рассылки, блоги, форумы, живые журналы, видеобиблиотеки (YouTube и др.), народные энциклопедии (Википедия и др.), IP-телефония, Skype, различные социальные сети.

Возможности и условия сети Интернет

Интернет является глобальной компьютерной сетью, которая охватывает весь мир и содержит огромный объем информации по любой тематике, доступной как на коммерческой, так и бесплатной основе, для всех желающих. Дополнительно к этому в сети Интернет можно произвести покупки и коммерческие сделки, оплатить счета, заказать билеты на различные виды транспорта, забронировать места в гостиницах и пр.

Различные информационные и поисковые системы используют разные способы организации данных и алгоритмы (средства) поиска нужной информации. Можно убедиться, что ввод одних и тех же ключевых слов в разные поисковые системы даст отличающиеся результаты.

В сети Интернет функционируют различные информационные системы, например:

- 1) World Wide Web (WWW) – Всемирная информационная паутина. Информация в данной системе состоит из страниц (документов). С помощью WWW можно смотреть фильмы, слушать музыку, играть в компьютерные игры, обращаться к различным информационным источникам;
- 2) FTP-система (File Transfer Program). Она используется для пересылки файлов, доступных для работы только после копирования на собственный компьютер пользователя;
- 3) электронная почта (E-mail). Каждый из абонентов обладает своим электронным адресом с «почтовым ящиком». Он представляет собой некоторый аналог почтового адреса. С помощью электронной почты пользователь способен пересылать и получать текстовые сообщения и двоичные файлы произвольного вида;
- 4) новости (система телеконференций – Use Net Newsgroups). Эта служба состоит из совокупности документов, сгруппированных по определенным темам;
- 5) IRC и ICQ - с помощью данных систем осуществляется обмен информацией в режиме реального времени. Эти функции в системе Windows выполняются приложением MS NetMeeting, которое позволяет создавать общие рисунки и добавлять текст совместно с

К средствам поиска, управления и контроля в Интернет относятся:

- системы поиска в WWW – используются для поиска информации, организованной одним из перечисленных выше способов (WWW, FTP);
- Telnet – режим удаленного управления любым компьютером в сети, применяемый для запуска на сервере или любом компьютере в Интернет необходимой программы;
- служебная программа Ping – позволяет проверять качество связи с сервером;
- программы Whois и Finger – используются для нахождения координат пользователей сети или определения пользователей, работающих в настоящий момент на конкретном хосте.

Для того чтобы система Интернет функционировала, требуется соответствующее программное обеспечение. Его можно разбить на две группы:

- универсальные программы (программные комплексы), которые обеспечивают доступ ко всем службам Интернет;
- специализированные программы, которые предоставляют наиболее широкие возможности для работы с каким-то одним (или группой) сервисом Интернет.

Разновидностью такого рода программ являются браузеры – специализированные программы для работы с интернет-сервисом WWW. Однако сегодня они поставляются обычно уже в виде комплекса программных средств, обеспечивающих все возможности работы в сети.

- Доступ в Интернет обычно получают через поставщиков услуг, называемых провайдерами (service provider). Для подключения к Интернет пользователь должен заключить контракт на обслуживание с любым из провайдеров, существующих в его регионе. Таким образом**, провайдер** – это юридическое лицо, обеспечивающее работу соответствующего сайта (узла), предоставляющего информационные услуги.
- Такого рода сайт (узел) фактически представляет из себя локальную сеть, которая включает в себя несколько компьютеров-серверов, применяемых для хранения информации определенного типа и в определенном формате. Каждому сайту и серверу на сайте присваиваются уникальные имена, с помощью которых они идентифицируются в сети Интернет.
- Провайдеры поставляют и продают различные виды интернет-услуг, каждый из них имеет свои преимущества и недостатки. Критериями оценки выбора того или иного провайдера могут служить цены, количество клиентов, характеристики внешних каналов, наличие дополнительных услуг и бесплатных сервисов.

Итак, для работы в Интернете необходимо выполнить следующие условия:

- физически подключить компьютер к одному из узлов Всемирной сети;
- получить IP-адрес на постоянной или временной основе;
- установить и настроить программное обеспечение (как минимум, набор программ-клиентов тех служб интернета, услугами которых предполагается пользоваться).

Для связи с провайдером и подключению к сети Интернет применяется обычно один из следующих способов:

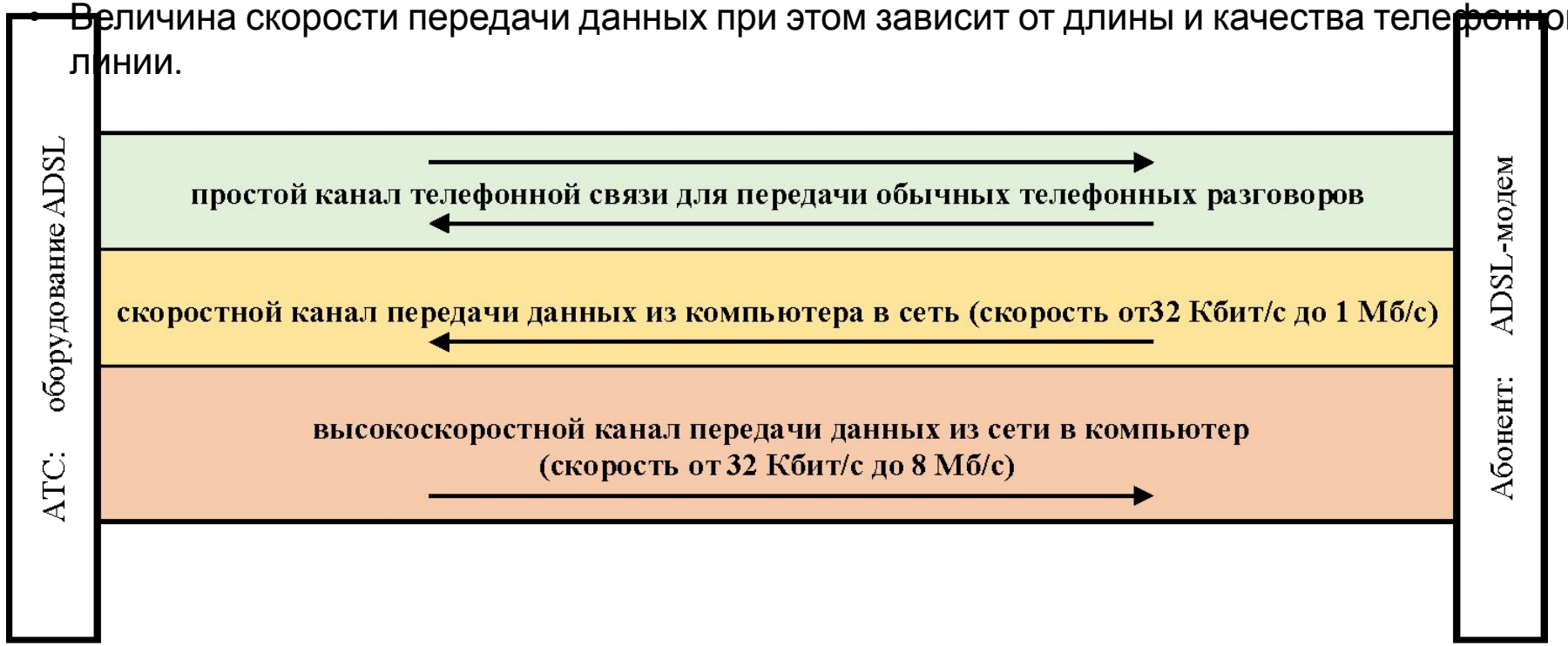
- коммутируемый доступ;
- выделенный доступ;
- беспроводной доступ.

Коммутируемый доступ. Этот вид доступа в Интернет – по коммутируемым линиям (Dial-Up) – является наиболее распространенным способом для частных пользователей.

- Коммутируемый – значит предоставляемый по каналам (линиям связи), не предназначенным специально для Интернета. Такими каналами связи выступают публичные телефонные сети, а для отграничения интернет-сигнала от телефонного сигнала используется специальное устройство – модем (модулятор/демодулятор).
- Модем необходим для преобразования цифровой информации, передаваемой участниками Интернета по коммутируемым линиям: несущие сигналы звуковой частоты модулируются по амплитуду, фазе и частоте. Естественно, что качество и скорость такой передачи прямо зависит от состояния телефонной линии и технических характеристик модема.

Коммутируемое соединение функционирует обычно на основе технологии **ADSL** (Asymmetric Digital Subscriber Line), обозначаемой как Асимметричная цифровая абонентская линия.

- Само название технологии подчеркивает изначально заложенное в ней различие скоростей обмена информацией в направлениях к абоненту и обратно. Это различие соответствует разным объемам информации: от абонента передаются небольшие объемы (в основном команды и запросы), а к абоненту – намного более крупные (видео, массивы данных, программы).
- Размещенное на АТС оборудование ADSL и абонентский ADSL-модем, подключаемые с разных концов телефонной линии, образуют таким образом три канала передачи данных (см. рис.)
- Величина скорости передачи данных при этом зависит от длины и качества телефонной линии.



Выделенный доступ – это постоянное соединение с Интернет по выделенной линии. Выделенная – значит специально предназначенная для передачи только интернет-сигнала.

- Данный способ работы наиболее совершенный, но и самый дорогой, поскольку требует прокладки специального кабеля. На предприятиях и в учреждениях обычно используют постоянное (выделенное) подключение к Интернету.
- Локальная сеть организации через шлюз подключена кабельным соединением непосредственно к узлу провайдера. В этом случае соединение с Всемирной сетью есть всегда и нет необходимости занимать телефонную линию для «дозвонки» до провайдера.
- Выделенное подключение имеет обычно большую пропускную способность и значительно более устойчиво, так как в нем отсутствуют помехи, свойственные телефонным сетям.

Беспроводной доступ. Все более широкое распространение получают различные беспроводные технологии передачи информации.

- Наиболее популярной их разновидностью сегодня является так называемая **Wi-Fi-технология.** С помощью этой технологии можно соединить компьютеры в одну сеть и/или подключиться к Интернету. Доступ в Интернет за небольшую плату может быть организован в публичных библиотеках, общественных учреждениях и так называемых Интернет-кафе. Некоторые городские власти и предприниматели предоставляют своим горожанам и соответственно клиентам бесплатный Wi-Fi-доступ в Интернет.
- Для этого в различных районах города размещаются так называемые хот-споты (точки доступа к Wi-Fi), в зоне покрытия которых пользователю необходимо находиться физически с тем, чтобы получать выход в Интернет. При этом компьютер клиента должен быть оснащен специальным устройством (адаптером, Wi-Fi-модемом, так называемой «карточкой» — для современных моделей ноутбуков).

Технологии Интернет

Информационные технологии постоянно увеличивают свое влияние на все сферы общественной жизни. Последняя треть XX столетия стала эпохой третьего машинного переворота, или третьей индустриальной революции. Сегодня интеллектуальная деятельность человека и совокупный интеллектуальный ресурс все больше выступают как машинный ресурс компьютерных сетей, тяготеющих к глобальному охвату.

В числе отличительных, имеющих стратегическое значение для развития экономики и общества в целом, существует семь наиболее важных.

- 1) Интернет-технологии позволяют активизировать и эффективно использовать информационные ресурсы общества, которые сегодня являются наиболее важным стратегическим фактором развития.
- 2) Интернет-технологии позволяют оптимизировать и во многих случаях автоматизировать информационные процессы, которые в последние годы занимают все большее место в жизнедеятельности человеческого общества.
- 3) Использование Интернет-технологий является элементом, включенным в более сложные производственные и социальные процессы. Поэтому зачастую Интернет-технологии выступают в качестве компонентов соответствующих производственных и социальных технологий.
- 4) Интернет-технологии сегодня играют исключительно важную роль в обеспечении информационного взаимодействия между людьми, а также в системах подготовки и распространения массовой информации.
- 5) Интернет-технологии занимают сегодня центральное место в процессе интеллектуализации общества и экономики.
- 6) Информационные технологии играют в настоящее время ключевую роль также и в процессах получения и накопления новых знаний.
- 7) Принципиально важное для современного этапа развития общества значение развития Интернет-технологий заключается в том, что их использование может оказать существенное влияние на решение основных проблем экономического развития общества.


Свойства информационных технологий (Интернет-технологий)
позволяют активизировать и эффективно использовать информационные ресурсы общества как наиболее важный стратегический фактор развития
их использование может оказать существенное влияние на решение основных проблем экономического развития общества
являются элементом более сложных производственных и социальных процессов, выступают в качестве компонентов производственных и социальных технологий
играют ключевую роль в процессах получения и накопления новых знаний
позволяют оптимизировать и автоматизировать информационные процессы, занимающие все большее место в жизнедеятельности человеческого общества
занимают центральное место в процессе интеллектуализации общества и экономики
играют исключительную роль в обеспечении информационного взаимодействия между людьми, а также в системах подготовки и распространения массовой информации

Компоненты Интернет-технологий могут быть рассмотрены с двух точек зрения: физической и логической.

- Базовую часть, техническое ядро Интернет-технологии образует так называемая опорная сеть Интерента с маршрутизаторами и шлюзами. Опорную сеть Интернета составляют узловые компьютеры (серверы, хосты) и каналы связи, объединяющие их между собой.
- На каждом из узлов работают маршрутизаторы, способные по IP-адресу принятого TCP-пакета автоматически определить, на какой из соседних узлов надо переправить этот пакет. Маршрутизатором может быть программа, но может быть и отдельный, специально выделенный для этой цели компьютер. Маршрутизатор непрерывно сканирует пространство соседних серверов, общается с их маршрутизаторами и потому знает состояние своего окружения. Он знает, когда какой-то из соседей «закрыт» на техническое обслуживание или просто перегружен. Принимая решение о переправке проходящего TCP-пакета, маршрутизатор учитывает состояние своих соседей и динамически перераспределяет потоки так, чтобы пакет ушел в том направлении, которое в данный момент наиболее оптимально.
- Шлюзы выполняют функцию «соединения несоединимого». Различные локальные сети, работающие на основе своих собственных протоколов (не TCP/IP, а других), подключаются к узловым компьютерам Интернета (работающих по интернет-протоколам TCP/IP) именно с помощью шлюзов. Роль шлюза может выполнять как особая программа, так и специальный компьютер. Таким образом, благодаря шлюзам происходит преобразование данных из форматов, принятых в

Физические компоненты Интернет-технологии

Сеть Интернет	• IP-адреса и протоколы TCP/IP • иерархическая система доменных имен (DNS) • опорная сеть Интернета и маршрутизация
Совокупность компьютеров (серверы и клиенты) в Интернете	• серверы электронной почты; • серверы телеконференций; • серверы мгновенных сообщений; • FTP-серверы; • Web-серверы.
Программное обеспечение в Интернете	• сетевые операционные системы; • специальное программное обеспечение для соединения с Интернетом; • прикладные протоколы
Доступ в Интернет	• соединение сетевой платы с локальной сетью • кабельные системы Ethernet • удаленный доступ к глобальным сетям • доступ "компьютер-сеть" • доступ "сеть-сеть"
Цифровые линии связи	• провайдеры и подключения

Физические и логические компоненты Интернет-технологий

- Интернет-технологии в физическом смысле – это совокупность взаимосвязанных компьютеров пользователей, локальных сетей организаций и узловых серверов, соединенных между собой различными каналами связи, а также специальное программное обеспечение, которое обеспечивает взаимодействие всех этих средств в системе "клиент-сервер", на основе единых стандартных протоколов.

- Рассмотрение Интернет-технологий в логическом смысле позволяет выделять те элементы информационного поля, которые оказывают непосредственное влияние на деятельность экономических агентов. Распределение информационных потоков создает условия для реализации новых проектов глобального характера. В тоже время происходит унификация основных логических компонентов Интернет-технологий, что создает дополнительные условия процессам глобализации экономики.

Логические компоненты Интернет-технологии

Интернет-сервисы	• электронная почта. Системы телеконференций • World Wide Web – Всемирная паутина • передача файлов (FTP) • передача мгновенных сообщений (ICQ) • интерактивное общение (чат, chat) • голосовое общение (IP-телефония) • аудио- и видеоконференции
Информационные ресурсы в Интернете	• URL-адресация и протоколы передачи данных • Web-страницы и Web-узлы, порталы. Web-пространство • создание Web-страниц. Языки Web-публикаций • публикации и представительство в Интернете
Инструменты для работы в Интернете	• браузеры • поисковые системы • навигация • лингвистические • прочие

Защита от сетевых угроз

Полная информационная безопасность в среде Internet невозможна в силу не только обретения последней глубокой «социальности», но и по самой природе Internet.

Она родилась как секретная корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства Internet объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и др., являющиеся по определению сетями с ограниченным доступом), но также и рядовых пользователей, которые имеют возможность получить прямой и недорогой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

Всё, что есть негативного в реальном обществе, имеется и в сети Интернет.

Защита сетей. В последнее время корпоративные сети все чаще включаются в Интернет или даже используют его в качестве своей основы. Учитывая, какой урон может принести незаконное вторжение в корпоративную сеть, разрабатываются соответствующей сложности методы защиты.

В этой связи выделяют следующие основные виды нарушения режима сетевой безопасности:

- угроза удаленного администрирования — несанкционированное управление удаленным компьютером;
- угроза активного содержимого — действия активных объектов, встроенных в web-страницы, которые включают в себя программный код, способный вести себя как компьютерный вирус;
- угроза перехвата или подмены данных на путях их транспортировки — например, при использовании карт платежных систем;
- угроза вмешательства в личную жизнь — возможность собирать и исследовать автоматизированными средствами предпочтения и вкусы пользователя без его ведома;
- угроза поставки неприемлемого содержимого — например, информации, которая не соответствует нормам морально-этического, религиозного или политического характера.

Основным решением для защиты корпоративных и других локальных сетей является использование брандмауэров.

- Брандмауэр (межсетевой экран, firewall) – это система или комбинация систем, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов данных из одной части сети в другую. Как правило, эта граница проводится между локальной сетью предприятия и Интернетом, хотя ее можно провести и внутри. Защищать отдельные компоненты не всегда целесообразно, поэтому обычно защищают всю сеть целиком.
- Брандмауэр пропускает через себя трафик и для каждого проходящего пакета принимает решение – пропускать его или отбросить. Для того, чтобы брандмауэр мог принимать такого рода решения, определяется набор четких правил. Брандмауэр может быть реализован как аппаратными средствами (как отдельное физическое устройство), так и в виде специальной программы, запущенной на компьютере. Брандмауэр считается наиболее надежным средством защиты информации от сетевых атак.
- В профилактических и мониторинговых целях защиты сетей используется сетевой аудит – протоколирование (запись) действий всех пользователей сети.

Защита информации. Проведение финансовых операций с использованием возможностей Интернета, заказ товаров и услуг, использование кредитных карточек, доступ к закрытым информационным ресурсам, передача телефонных разговоров – все эти стороны человеческой деятельности требуют поддержания соответствующего уровня безопасности.

- Для обеспечения секретности применяется шифрование (криптография), позволяющее трансформировать данные в зашифрованную форму (криптографически преобразовать информацию), из которой исходную информацию можно извлечь только с помощью ключа. В основе шифрования лежат два основных понятия: **алгоритм и ключ**.
- Алгоритм шифрования – это способ закодировать исходный текст. Получившееся зашифрованное послание может быть интерпретировано (прочитано) только с помощью ключа, представляющего собой последовательность битов.

- Существуют две схемы шифрования:
  - симметричное шифрование (традиционное) – шифрование с закрытым ключом;
  - асимметричное шифрование – шифрование с открытым ключом.
- При симметричном шифровании отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровать и расшифровывать данные. Таким образом, ключом владеют два человека.
- В схеме шифрования с открытым ключом используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго – расшифровывается. Первый ключ делается общедоступным (публичным). Второй ключ хранится только у получателя информации, он является закрытым. Здесь ключом расшифровки владеет только один человек.

- Дополнительно к этому, для идентификации личности отправителя сообщения применяется электронно-цифровая подпись (ЭЦП) как некая определенная последовательность символов, в которой используется сжатый образ исходного текста. Благодаря этой особенности ЭЦП позволяет однозначно связать между собой следующие три атрибута сообщения:
  - автор документа,
  - содержание документа,
  - владелец ЭЦП.

Вредоносные программы

- Массовое применение компьютеров оказалось связанным с появлением самовоспроизводящихся и других вредоносных программ (вредоносных кодов), препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Проникнув в один компьютер, такие программы способны распространиться на другие компьютеры.
- В соответствии со способами распространения и вредоносной нагрузкой все вредоносные программы можно подразделить на:
  - вирусы,
  - черви,
  - трояны,
  - прочие программы.

Вирус (компьютерный вирус) – это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты.

- Компьютерные вирусы обладают тремя отличительными особенностями:

  - несамостоятельность – вирусы могут распространяться только благодаря действиям человека. То есть, вирус может попасть на другой компьютер только в том случае, если пользователь отправит на него зараженный вирусом файл, например, посредством электронной почты;

  - саморазмножение – вирус создает свои собственные копии, способные к дальнейшему распространению;

  - специализация – вирусы жестко привязаны к той операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Это означает, что вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например Unix. Точно также макровирус для Microsoft Word 2003 не будет, скорее всего, работать в приложении Microsoft Excel 97.

- Основные цели любого компьютерного вируса – это распространение на другие ресурсы компьютера и выполнение специальных действий (в том числе, вредоносных) при определенных событиях или действиях пользователя (например, 23 числа каждого четного месяца или при перезагрузке компьютера).

- Жизненный цикл любого компьютерного вируса можно разделить на пять стадий:
  1. Проникновение на чужой компьютер,
  2. Активация,
  3. Поиск объектов для заражения,
  4. Подготовка копий,
  5. Внедрение копий.

- После проникновения на компьютер, вирус должен активироваться, т. е. быть запущенным к исполнению. По месту дислокации такого запуска вирусы делятся на:

  А. Загрузочные вирусы – заражают загрузочные сектора жестких дисков и мобильных носителей,

  Б. Файловые вирусы – заражают именно файлы. В этой группе вирусов выделяют две разновидности по типу среды обитания:

  б1. Классические файловые вирусы – они различными способами внедряются в исполняемые файлы (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы;

  б2. Макровирусы, которые написаны на внутреннем языке какого-либо приложения, с помощью так называемых макросов. Подавляющее большинство макровирусов используют макросы текстового редактора Microsoft Word.

Создаваемые вирусом копии маскируются, чтобы уберечь их от действия антивирусных программ. По технологиям маскировки вирусы разделяются на:

- шифрованные – в этом случае вирус состоит из двух частей: сам вирус и шифратор;
- метаморфные – здесь копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд;
- полиморфные – используются комбинации обоих типов маскировки.

Червь (сетевой червь) – это вредоносная программа, самостоятельно распространяющаяся по сетевым каналам и способная к преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом. Цели червей связаны с нанесением ущерба нормальному функционированию различных сетевых объектов.

Жизненный цикл червей состоит из стадий, подобных вирусам, но в отличие от вирусов черви – это вполне самостоятельные программы: размножившись, они не ждут действий пользователя, а сами начинают распространяться по сети. От пользователей червю иногда требуется, чтобы его активировали.

По методу активации черви делятся на:

- требующие активного участия пользователя;
- полностью автономные;

В первом случае черви используют методы обмана. Это проявляется, например, когда получатель инфицированного файла вводится в заблуждение интригующим текстом письма и добровольно открывает вложение с почтовым червем, тем самым его активируя.

Во втором случае черви активируются сами, используя ошибки в настройке операционной системы или бреши в ее системе безопасности.

В третьем случае действия пользователя дают добавочный позитивный импульс процессу самоактивации червей, ускоряя его. Такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Дополнительно к этому сетевые черви могут кооперироваться с вирусами. Такая вредоносная «пара» способна самостоятельно распространяться по сети (благодаря червю) и одновременно – заражать ресурсы компьютера (функции вируса).

Троян – вредоносная программа, основной особенностью которой является ее маскировка под полезное приложение.

Трояны, или программы класса «троянский конь», в отличие от вирусов и червей не обязаны уметь размножаться. Это программы, написанные только с одной целью – нанести ущерб конкретному компьютеру путем выполнения различных, не санкционированных пользователем, действий:

- кража, порча или удаление конфиденциальных данных;
- нарушение нормальной работоспособности компьютера;
- использование ресурсов компьютера в неблаговидных целях.

Жизненный цикл троянов состоит из трех стадий:

1. Проникновение в систему,
2. Активация,
3. Выполнение вредоносных действий.

Особенности проникновения троянов в компьютер:

- всегда – обязательная маскировка – троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернета) и запускает. При этом сама программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные трояну;
- в большинстве случаев – кооперация – троянские программы проникают на компьютеры вместе с вирусом либо червем;
- иногда – автономность – некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы.

Разновидности троянов по типу вредоносной нагрузки:

- клавиатурные шпионы – постоянно находясь в оперативной памяти, трояны записывают все данные (сигналы), поступающие от клавиатуры, с целью последующей передачи их своему заказчику;
- похитители паролей – предназначены для кражи паролей путем поиска на компьютере специальных файлов, которые их содержат;
- организаторы атак – эти трояны, не нарушая работоспособности инфицированного компьютера, наносят вред другим, удаленным компьютерам и сетям (например, при так называемых DDoS-атаках).

Защита компьютеров

К основным признакам проявления вредоносного действия можно отнести:

- прекращение работы или неправильная работа ранее успешно функционирующих программ и устройств;
- медленная работа компьютера, частые зависания и сбои;
- невозможность загрузки операционной системы;
- исчезновение файлов и папок или искажение их содержимого;
- изменение размеров, даты и времени модификации файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов.

Вышеперечисленные явления не обязательно вызываются присутствием вредоносного кода, а могут быть следствием других причин. Поэтому диагностика состояния компьютера всегда затруднена. Эффективным средством считаются специальные программы, называемые антивирусными.

Антивирусные программы – это программы для защиты от компьютерных вирусов, червей, троянов и других вредоносных программ, а также для их обнаружения и удаления.

Все используемые в настоящее время антивирусные программы подразделяются на пять типов в соответствии с их назначением:

- ревизоры – постоянно сравнивают текущие состояния компонентов компьютерной системы с предыдущими в целях выявления подозрительных отклонений;
- сканеры – осуществляют поиск и лечение зараженных вирусами объектов широким спектром приемов от простейшего помещения в карантин (изоляцию) до уничтожения;
- мониторы (сторожа, фильтры) – не пропускают вредоносные объекты, действуя на входных потоках информации;
- иммунизаторы – имитируют зараженность здоровых файлов, в результате чего вирус начинает считать их уже «больными» и не заражает;
- блокираторы – идентифицируют подозрительные программы по их характерному поведению и останавливают (блокируют) их выполнение.

Выбор системы антивирусного противодействия обусловлен материальными возмож-ностями, особенностями работы защищаемого объекта и перечнем решаемых задач.

Наиболее известные из современных антивирусных программ (Kaspersky, DrWeb, NOD32 и др.) являются универсальными и сочетают в себе в той или иной мере не только перечисленные функции, но и некоторые другие, связанные с взаимодействием с операционной системой (ОС) и предоставлением пользователю иных подобных дополнительных удобств (отслеживают, например, регулярность загрузки и установки обновлений ОС).

Спасибо за внимание!