ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
(ТПУ)

КАФЕДРА ПРИКЛАДНОЙ МАТЕМАТИКИ (ПМ)

ИНФОРМАТИКА

Лектор: к.т.н., доцент кафедры ПМ, Зимин Вячеслав Прокопьевич

Лабораторные занятия ведут:
к.т.н., доцент кафедры ПМ, Вадутова Фаина Александровна
старший преподаватель кафедры ПМ, Крылова Лариса Михайловна
к.т.н., доцент кафедры ПМ, Зимин Вячеслав Прокопьевич

ТЕМА 6.
ЛОКАЛЬНЫЕ И ГЛОБАЛЬНЫЕ СЕТИ ЭВМ.
ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ

1. Сетевые технологии обработки данных.

2. Принципы организации и основные топологии вычислительных сетей.

3. Сетевой сервис и сетевые стандарты.

4. Защита информации в локальных и глобальных компьютерных сетях.

АВТОНОМНЫЙ ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР В СОСТАВЕ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Для работы автономного ПК в составе вычислительной сети необходимы дополнительные устройства: модемы, дополнительные платы и линии связи, связывающие компьютеры друг с другом и дополнительное программное обеспечение.
Модем необходим для организации работы через телефонные сети.
Сетевой адаптер предназначен для организации работы в составе локальной вычислительной сети.

<u>Классификация вычислительных сетей</u>

1. Локальные вычислительные сети (ЛВС, LAN).
2. Корпоративные вычислительные сети (КВС, CAN).
3. Городские вычислительные сети (ГрВС, MAN).
4. Региональные вычислительные сети (РВС, DAN).
5. Глобальные вычислительные сети (ГВС, WAN).

Основу практически всех вычислительных сетей составляют <u>локальные вычислительные сети</u>.

ОПРЕДЕЛЕНИЯ ПОНЯТИЙ ЛВС

Отличительные признаки локальной вычислительной сети можно сформулировать следующим образом:

1. Высокая скорость передачи информации, большая пропускная способность сети. Приемлемая скорость в настоящее время — не менее 10 Мбод (1 бит/с. = 1бод).

2. Низкий уровень ошибок передачи (или, что тоже самое, высококачественные каналы связи). Допустимая вероятность ошибок передачи данных должна быть порядка 10^{-8} — 10^{-12}.

3. Эффективный, быстродействующий механизм управления обменом информации по сети.

4. Заранее четко ограниченное количество компьютеров, подключаемых к сети.

Компьютеры, связанные локальной вычислительной сетью, объединяются в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем к ресурсам, входящим непосредственно в каждый отдельный компьютер.

ОПРЕДЕЛЕНИЯ ПОНЯТИЙ, СВЯЗАННЫХ С ЛВС

Абонент (узел, хост, станция) — это устройство, подключенное к сети и активно участвующее в информационном обмене. Чаще всего абонентом (узлом) сети является компьютер, но абонентом также может быть, например, сетевой принтер или другое периферийное устройство, имеющее возможность напрямую подключаться к сети (т.е. имеющее собственный IP-адрес). Далее в курсе вместо термина «абонент» для простоты будет использоваться термин «компьютер».

Сервером называется абонент (узел) сети, который предоставляет свои ресурсы другим абонентам, но сам не использует их ресурсы. Таким образом, сервер обслуживает сеть. Серверов в сети может быть несколько, и совсем не обязательно, что сервер — самый мощный компьютер. Выделенный сервер (dedicated server)— это сервер, занимающийся только сетевыми задачами. Невыделенный сервер может помимо обслуживания сети выполнять и другие задачи. Специфический тип сервера — это сетевой принтер.

Клиентом называется абонент сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает, то есть сеть его обслуживает, а он ей только пользуется. Компьютер-клиент также часто называют рабочей станцией. В принципе каждый компьютер сети может быть одновременно как клиентом, так и сервером и такие сети называются одноранговыми.

Под сервером и клиентом часто понимают также не сами компьютеры, а работающие на них программные приложения. В этом случае то приложение, которое только отдает ресурс в сеть, является сервером, а то приложение, которое только пользуется сетевыми ресурсами — клиентом.

ТОПОЛОГИЯ ЛВС

Топология (компоновка, конфигурация, структура) компьютерной сети – это физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи.

Топология определяет:

1) требования к оборудованию;

2) тип используемого кабеля;

3) допустимые и наиболее удобные методы управления обменом;

4) надежность работы сети;

5) возможности расширения сети.

Базовые топологии сети:

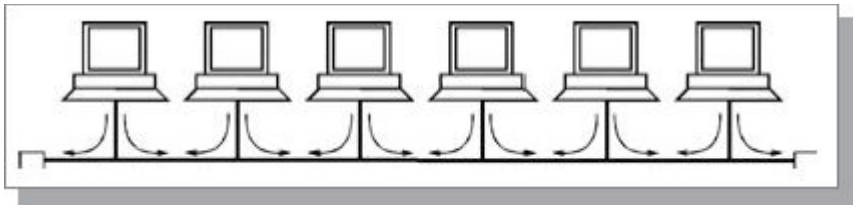
1. Шина.

2. Звезда.

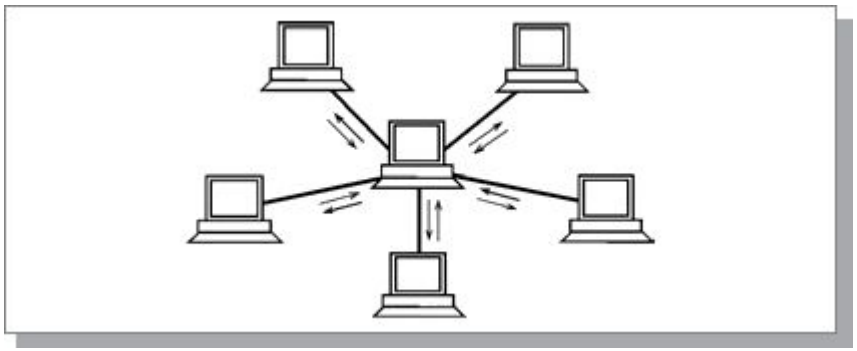
3. Кольцо.

ТОПОЛОГИЯ ЛВС

Шина (bus) — все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компьютера одновременно передается всем остальным компьютерам.

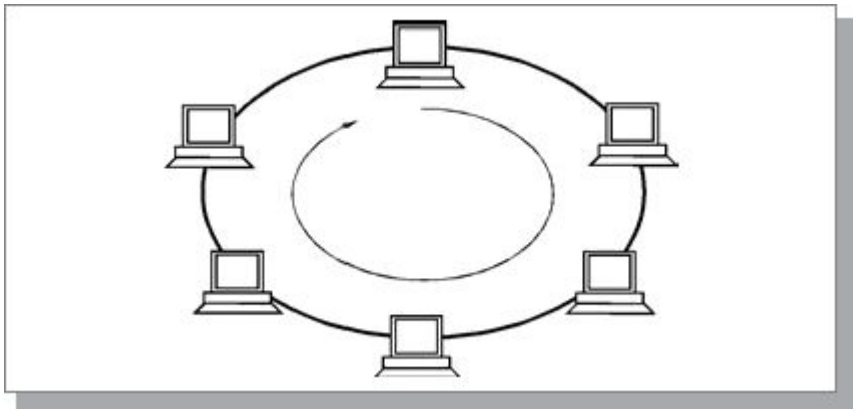


Звезда (star) — к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует отдельную линию связи. Информация от периферийного компьютера передается только центральному компьютеру, от центрального — одному или нескольким периферийным.



ТОПОЛОГИЯ ЛВС

Кольцо (ring) — компьютеры последовательно объединены в кольцо. Передача информации в кольце всегда производится только в одном направлении. Каждый из компьютеров передает информацию только одному компьютеру, следующему в цепочке за ним, а получает информацию только от предыдущего в цепочке компьютера.



ТОПОЛОГИЯ ЛВС

Факторы, влияющие на физическую работоспособность сети и непосредственно связанные с понятием топология.

1. Исправность компьютеров (абонентов), подключенных к сети. В некоторых случаях поломка абонента может заблокировать работу всей сети. Иногда неисправность абонента не влияет на работу сети в целом, не мешает остальным абонентам обмениваться информацией.

2. Исправность сетевого оборудования, то есть технических средств, непосредственно подключенных к сети (адаптеры, трансиверы, разъемы и т.д.). Выход из строя сетевого оборудования одного из абонентов может сказаться на всей сети, но может нарушить обмен только с одним абонентом.

3. Целостность кабеля сети. При обрыве кабеля сети (например, из-за механических воздействий) может нарушиться обмен информацией во всей сети или в одной из ее частей. Для электрических кабелей столь же критично короткое замыкание в кабеле.

4. Ограничение длины кабеля, связанное с затуханием распространяющегося по нему сигнала. Как известно, в любой среде при распространении сигнал ослабляется (затухает). И чем большее расстояние проходит сигнал, тем больше он затухает. Необходимо следить, чтобы длина кабеля сети не была больше предельной длины $L_{пр}$, при превышении которой затухание становится уже неприемлемым (принимающий абонент не распознает ослабевший сигнал).

ТОПОЛОГИЯ ЛВС

В общем случае, при упоминании о топологии сети, подразумевается четыре совершенно разные понятия, относящиеся к различным уровням сетевой архитектуры:

1. Физическая топология (географическая схема расположения компьютеров и прокладки кабелей). В этом смысле, например, пассивная звезда ничем не отличается от активной, поэтому ее нередко называют просто звездой.

2. Логическая топология (структура связей, характер распространения сигналов по сети). Это наиболее правильное определение топологии.

3. Топология управления обменом (принцип и последовательность передачи права на захват сети между отдельными компьютерами).

4. Информационная топология (направление потоков информации, передаваемой по сети).

ЛИНИИ СВЯЗИ ЛВС

Среда передачи информации - это линии связи (или каналы связи), по которым производится обмен информацией между компьютерами.

Классификация линий связи:

1. Проводные или кабельные каналы связи (провода, витая пара, коаксиальный кабель, оптоволоконный кабель).

2. Беспроводные лини связи.

Каждый тип лини связи имеет свои преимущества и недостатки. Поэтому при выборе надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию ЛВС.

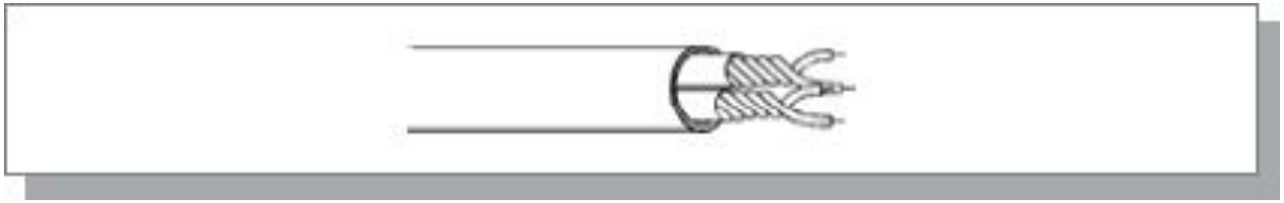
Основные параметры линий связи, наиболее важные для использования в локальных сетях:

1. Полоса пропускания линий связи (частотный диапазон сигналов, пропускаемых линией связи).

2. Затухание сигнала в линии связи.

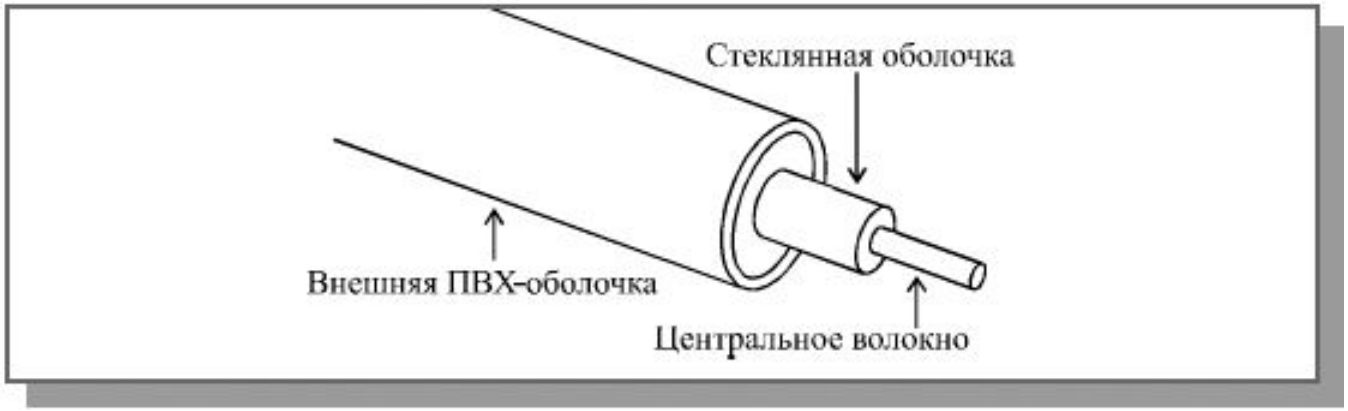
ЛИНИИ СВЯЗИ ЛВС

Кабель с витыми парами



Коаксиальный кабель

Оптоволоконный кабель



СЕТЕВОЙ СЕРВИС

Сетевые сервисы и обеспечивающие их протоколы:

1. Удаленный доступ к ЭВМ. Протокол Telnet.

2. Удаленный доступ к файлам. Протоколы File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) и Network File System (NFS).

3. Организация электронной почты. Протокол Simple Mail Transfer Protocol (SMTP).
Пример. Адрес e-mail Иванова И.И. сотрудника ИДО ТПУ:
`ivanov@ido.tpu.ru`

4. Доступ к web-ресурсам. Служба имен доменов (DNS).
Пример. Адрес сайта Института «Кибернетический центр» ТПУ:
`http://www.cctpu.edu.ru`

В ассоциации сетей Internet используются протоколы TCP/IP.

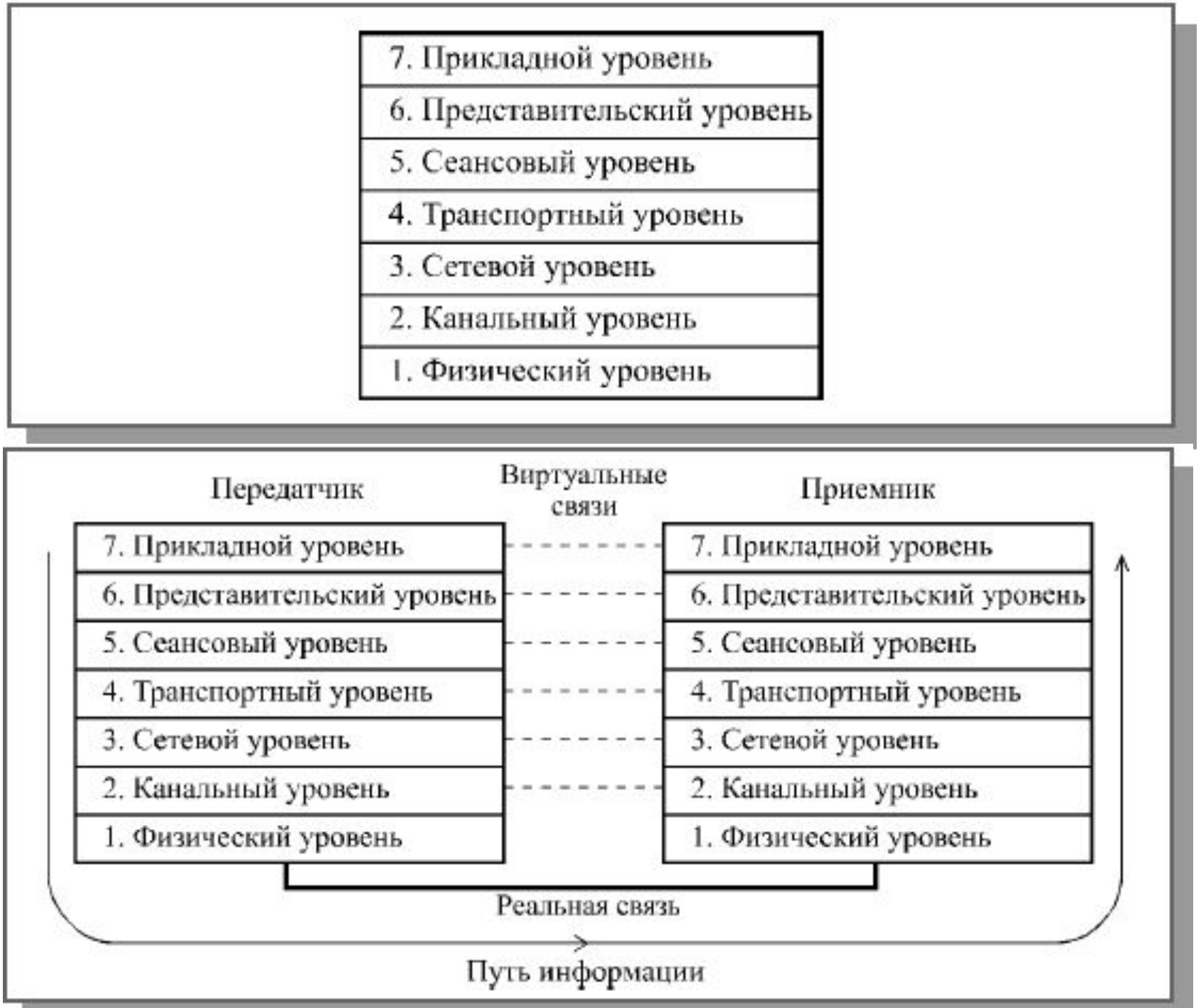
СЕТЕВЫЕ СТАНДАРТЫ

МОДЕЛЬ OSI/ISO

Наибольшее распространение при анализе операций, обеспечивающих передачу данных от компьютера к компьютеру, получила так называемая эталонная модель обмена информацией открытой системы OSI (Open System Interchange). Эта модель разработана в 1984 году Международным институтом стандартизации ISO (International Standards Organization), поэтому модель называют OSI/ISO.

Все сетевые функции в модели разделены на 7 уровней. При этом вышестоящие уровни выполняют более сложные, глобальные задачи, для чего используют в своих целях нижестоящие уровни, а также управляют ими. Цель нижестоящего уровня – предоставление услуг вышестоящему уровню, причем вышестоящему уровню не важны детали выполнения этих услуг. Нижестоящие уровни выполняют более простые и конкретные функции. В идеале каждый уровень взаимодействует только с теми уровнями, которые находятся рядом с ним (выше и ниже него). Верхний уровень соответствует прикладной задаче, работающему в данный момент приложению, нижний – непосредственной передаче сигналов по каналу связи.

Между одинаковыми уровнями передатчика и приемника существует виртуальная (или реальная) связь, которая реализуется с помощью протоколов соответствующих уровней.


7. Прикладной уровень
6. Представительский уровень
5. Сеансовый уровень
4. Транспортный уровень
3. Сетевой уровень
2. Канальный уровень
1. Физический уровень
Передатчик
Виртуальные связи
Приемник
7. Прикладной уровень
6. Представительский уровень
5. Сеансовый уровень
4. Транспортный уровень
3. Сетевой уровень
2. Канальный уровень
1. Физический уровень
7. Прикладной уровень
6. Представительский уровень
5. Сеансовый уровень
4. Транспортный уровень
3. Сетевой уровень
2. Канальный уровень
1. Физический уровень
Реальная связь
Путь информации

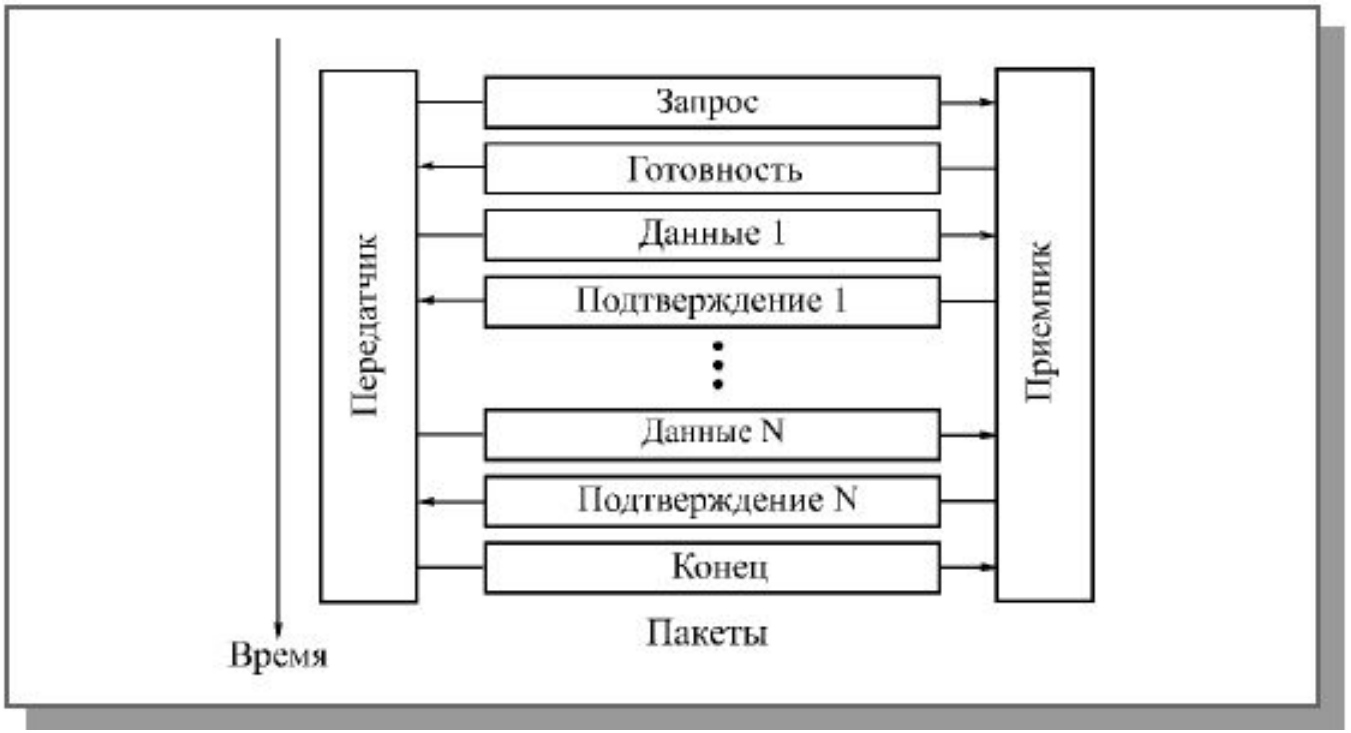
МОДЕЛЬ ПЕРЕДАЧИ ДАННЫЙ В INTERNET

Реально в разнообразных вычислительных сетях обычно используются не все 7 уровней. Так, например, в сети Internet наиболее часто используются 2 уровня. (соответственно, 2 протокола).

Транспортный уровень – протокол управления передачей (Transmitting Control Protocol, TCP).

Сетевой уровень – межсетевой протокол (Internet protocol, IP).

С помощью этих двух протоколов между приемником и передатчиком осуществляется связь посредством передачи/приёма данных (пакетов).



ПРОЕКТ 802

Помимо модели OSI существует также модель IEEE Project 802, принятая в феврале 1980 год, которую можно рассматривать как модификацию, развитие, уточнение модели OSI.

Стандарты, определяемые этой моделью (так называемые 802-спецификации) относятся к нижним двум уровням модели OSI и делятся на двенадцать категорий, каждой из которых присвоен свой номер.

ПРОЕКТ 802

802.1 – объединение сетей с помощью мостов и коммутаторов.
802.2 – управление логической связью на подуровне LLC.
802.3 – локальная сеть с методом доступа CSMA/CD и топологией шина (Ethernet).
802.4 – локальная сеть с топологией шина и маркерным доступом (Token-Bus).
802.5 – локальная сеть с топологией кольцо и маркерным доступом (Token-Ring).
802.6 – городская сеть (Metropolitan Area Network, MAN) с расстояниями между абонентами более 5 км.
802.7 – широкополосная технология передачи данных.
802.8 – оптоволоконная технология.
802.9 – интегрированные сети с возможностью передачи речи и данных.
802.10 – безопасность сетей, шифрование данных.
802.11 – беспроводная сеть по радиоканалу (WLAN – Wireless LAN).
802.12 – локальная сеть с централизованным управлением доступом по приоритетам запросов и топологией звезда (100VG-AnyLAN).

ПРОЕКТ 802

В первую очередь данный проект определил правила построения и функционирования, а также оборудование таких локальных сетей как:

1. Ethernet.
2. Arcnet.
3. Token Ring.

В настоящее время широко используются сети:

1. Fast Ethernet (100 Мбит/с).
2. Gigabit Ethernet (1000 Мбит/с).
3. High Speed Token-Ring, HSTR (100 Мбит/с).
4. Gigabit Token-Ring (1000 Мбит/с).

ЗАЩИТА ИНФОРМАЦИИ В ЛОКАЛЬНЫХ И ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, несанкционированного доступа (НСД) блокирования информации и т.п.

Наряду с термином «защита информации» (применительно к компьютерным сетям) широко используется, как правило, в близком значении, термин «компьютерная безопасность».

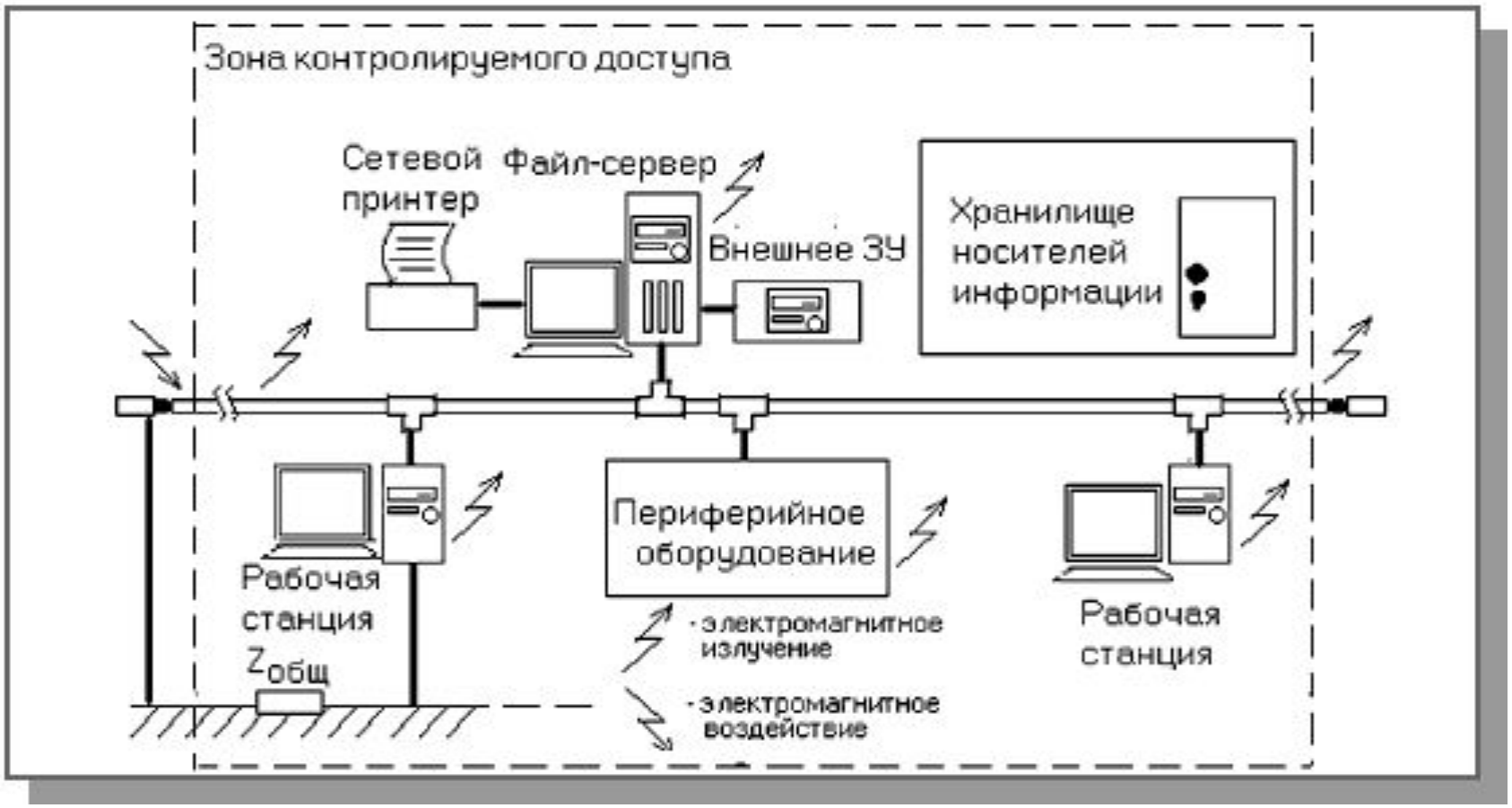
Переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам:

1) большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц;

2) значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть;

3) недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предпродажном этапе, называемом бета-тестированием, а в процессе эксплуатации. В том числе неидеальны встроенные средства защиты информации даже в таких известных и сетевых ОС, как MS Windows или NetWare.

МЕСТА И КАНАЛЫ ВОЗМОЖНОГО НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ СЕТИ



СПОСОБЫ РЕАЛИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи *защиты информации*. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую – упоминавшиеся выше генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные *каналы утечки информации* или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

СПОСОБЫ РЕАЛИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ (продолжение)

3. Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

Наиболее распространёнными являются программные средства защиты информации.

1. Шифрование данных, использование криптографии.
2. Использование такой процедуры как конфиденциальность – защищенность информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В свою очередь аутентификация представляет собой установление подлинности различных аспектов информационного взаимодействия: сеанса связи, сторон (идентификация), содержания (имитозащита) и источника (установление авторства с помощью пароля, цифровой подписи, отпечатков пальцев, голоса, радужной оболочки глаза и т.д.).

МЕТОДЫ ШИФРОВАНИЯ

Базовые методы шифрования:

1) подстановка (простая – одноалфавитная, многоалфавитная однопетлевая, многоалфавитная многопетлевая);

2) перестановка (простая, усложненная);

3) гаммирование (смешивание с короткой, длинной или неограниченной маской).

Подстановка предполагает использование альтернативного алфавита (или нескольких) вместо исходного. В случае простой подстановки для символов английского алфавита можно предложить, например, следующую замену.

Пример замены символов при подстановке

Исходный алфавит	**A B C D E F G H I J K L … X Y Z**
Альтернативный алфавит	**S O U H K T L X N W M Y … A P J**

Тогда слово «hi» в зашифрованном виде представляется как «xn».