**Дисциплина: «Компьютерные сети»**

**Преподаватель: Суягин Михаил Алексеевич**

1. **NAT**

<https://habr.com/ru/articles/583172/>

Нехватка айпишников. Технология нат

В 80х годах ХХ века заложили основу IPv4, позволяющую создавать ~4.3 млрд. адресов, но никто не предполагал, что этот запас так быстро иссякнет. С каждым годом появлялось все больше и больше пользователей и с 25 ноября 2019г. в России и в Европе официально закончились [IP адреса](https://timeweb.com/ru/community/articles/v-rossii-i-evrope-zakonchilis-ip-adresa-protokola-ipv4). Лимит исчерпан.

Для решения этой проблемы было придумано несколько способов:  
Первый способ заключается в усилении **контроля** за IP адресами.

Второй способ - в массовом использовании системы **IPv6**.

И третий способ - использование технологии трансляции сетевых адресов - **NAT**.

<https://cloudlite.ru/faq/chto-takoe-nat-i-zachem-on-nuzhen/>

**NAT (Network Address Translation)** – технология преобразовывания приватных IP-адресов во внешние в IPv4. Благодаря этому процессу ваша виртуальная машина получает доступ в Интернет.

В частной сети используются приватные (серые) IP-адреса, которые не используются в Интернете. Группой проектирования Интернета в 1994 были выбраны следующие подсети (что остаётся актуальным и по сей день):

В результате для внутреннего применения были зарезервированы три блока IP-адресов:

10.0.0.0 – 10.255.255.255/8 (16777216 хостов)

172.16.0.0 – 172.31.255.255/12 (1048576 хостов)

192.168.0.0 – 192.168.255.255/16 (65536 хостов)

Частные IP-адреса, также называемые внутренними, внутрисетевыми, локальными или серыми, любая организация имеет право использовать по своему усмотрению без всякой регистрации у какой-либо организации.

Чтобы выходить в Интернет нужен белый IP, который будет «маскировать» 1 или несколько приватных IP-адресов.

Механизм NAT как раз осуществляет подмену (или «маскировку») серых адресов на белые и наоборот.

Таким образом, вся частная сеть может подключаться к Интернету через один публичный IP-адрес (или пул адресов), предоставленный провайдером. В результате, ресурс глобальных адресов расходуется гораздо экономнее.

Преобразования NAT имеет важную особенность с точки зрения обеспечения безопасности: трансляция частных IP-адресов в публичные из пула маршрутизатора, позволяет скрыть топологию внутренней сети от внешних пользователей, что затрудняет несанкционированный доступ к ресурсам сети.

1. **Межсетевой экран. Назначение, принципы работы**

<https://selectel.ru/blog/firewall/>

Межсетевой экран (МЭ, брандмауэр или Firewall) представляет собой программно-аппаратный или программный комплекс, который отслеживает сетевые пакеты, блокирует или разрешает их прохождение. В фильтрации трафика брандмауэр опирается на установленные параметры — чаще всего их называют правилами МЭ.

Современные межсетевые экраны располагаются на периферии сети, ограничивают транзит трафика, установку нежелательных соединений и подобные действия за счет средств фильтрации и аутентификации.



Главная задача МЭ – это фильтрация трафика между зонами сети. Он может использоваться для разграничения прав доступа в сеть, защиты от сканирования сети компании, проведения сетевых атак. Проще говоря, межсетевой экран – это одно из устройств, при помощи которого обеспечивается сетевая безопасность компании.

## Как работает межсетевой экран

Если взять простой пример, то брандмауэр напоминает бдительного охранника, который знает в лицо миллионы потенциальных преступников. Он осматривает всех людей, входящих в здание, и если видит среди них одного из злоумышленников, то не впускает его внутрь. Аналогично работает брандмауэр, обеспечивая мониторинг и регулирование трафика, входящего и исходящего из вашей сети. Это достигается с помощью различных методов, включая фильтрацию пакетов, прокси-сервис и проверку с отслеживанием состояния. Помимо этого, файрвол может предотвратить использование системы злоумышленником для распространения вредоносного кода.

1. **Протокол OSPF**

<https://selectel.ru/blog/ospf/>

OSPF расшифровывается как Open Shortest Path First. Если переводить дословно, получится что-то вроде «открытый короткий путь первым». Под названием скрывается протокол внутренней маршрутизации, который передает информацию по лучшему пути. Но, несмотря на название, он не всегда короткий. Чтобы найти лучший путь, протокол отслеживает состояние каналов, а путь рассчитывается по алгоритму Дейкстры.

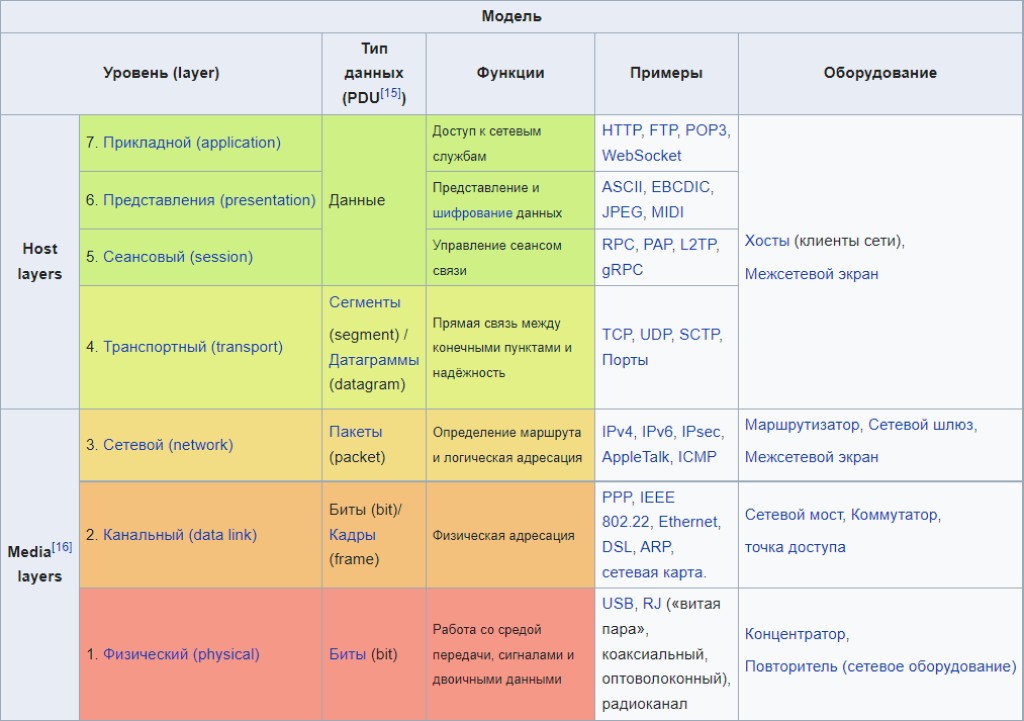
OSPF довольно просто настраивается по инструкциям, но вот объяснить порядок его работы довольно сложно. Попробуем это сделать.

Протокол OSPF заполняет таблицы маршрутизации автоматически, при этом маршрутизаторы постоянно обмениваются данными о состоянии сети и актуализируют таблицу. Администратору не нужно бегать и самостоятельно переписывать таблицы.

Аналогично в случае сбоев: со статической маршрутизацией тяжело отслеживать доступность сетей. Если канал между маршрутизаторами прерван, то пакеты, которые M2 получил от M1 (см. схему ниже), никуда не отправятся.

1. **Модель OSI**

<https://selectel.ru/blog/osi-for-beginners/>



1. **LAN**

<https://wiki.merionet.ru/articles/chto-takoe-lan-i-chem-otlichaetsya-ot-wan/>

Лока́льная вычисли́тельная сеть (ЛВС, локальная сеть; англ. Local Area Network, LAN) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).

1. **Протокол RIP. Описание, принцип работы**

<https://www.ibm.com/docs/ru/i/7.1?topic=routing-information-protocol>

*Протокол информации о маршрутизации* (RIP) - это протокол дистанционно-векторной маршрутизации. Маршрутизаторы, работающие через этот протокол, отправляют всю или часть своей таблицы маршрутизации соседям в сообщении для обновления.

RIP позволяет настраивать хосты в качестве узлов сети RIP. Процедура настройки такого способа маршрутизации достаточно проста. Кроме того, он обеспечивает автоматическое обновление таблиц маршрутизации при изменении сети или остановке сетевой связи. В System i применяется протокол RIPv2, позволяющий обновлять настроенные в сети маршруты путем обмена пакетами RIP.

1. **Статическая маршрутизация**

[**https://www.ibm.com/docs/ru/aix/7.2?topic=routing-static-dynamic**](https://www.ibm.com/docs/ru/aix/7.2?topic=routing-static-dynamic)

Статическая маршрутизация – вид маршрутизации, при котором информация о маршрутах заносится в таблицы маршрутизации каждого маршрутизатора вручную администратором сети.

Статическая маршрутизация означает, что таблицы маршрутизации обслуживаются вручную с помощью команды **route**. Этот тип маршрутизации рекомендуется применять тогда, когда ваша сеть взаимодействует с одной или двумя другими сетями. Однако если сеть соединена с большим числом сетей, то число шлюзов резко возрастает, и для обслуживания таблиц маршрутизации вручную требуется значительное время.

1. **Протокол DHCP**

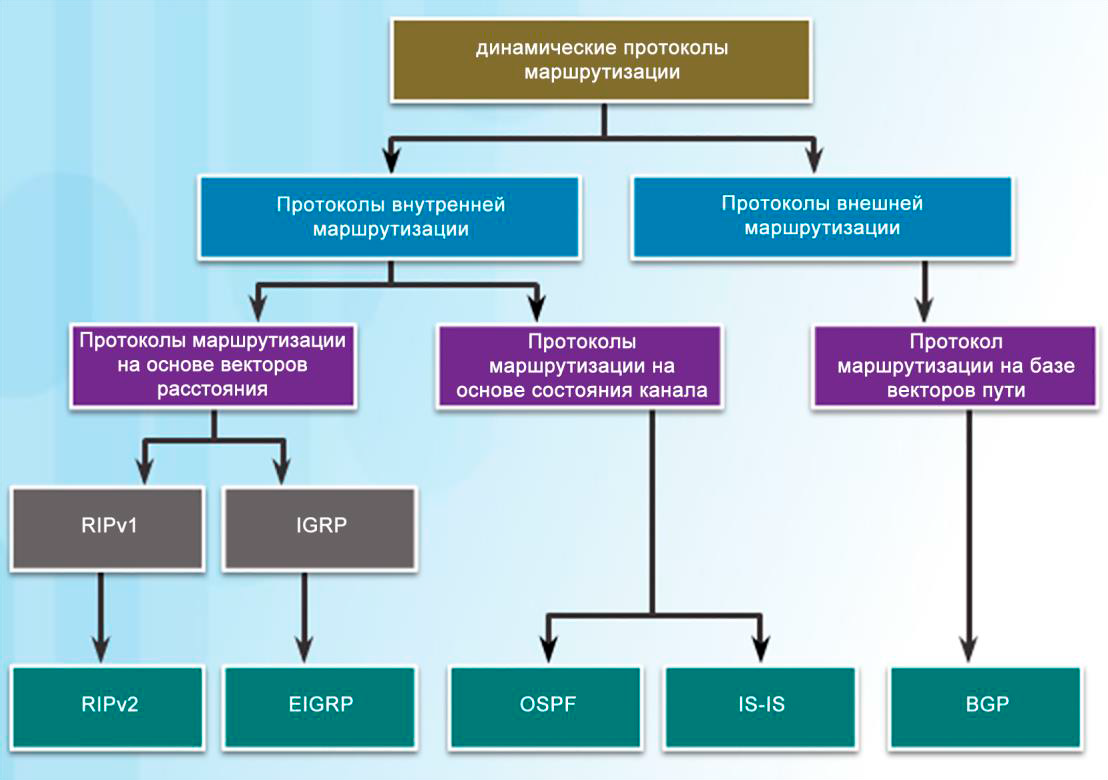
[**https://selectel.ru/blog/dhcp-protocol/**](https://selectel.ru/blog/dhcp-protocol/)

DORA DISCOVERY OFFER REQUEST ACK

1. **Динамическая маршрутизация**

Динамическая маршрутизация – это вид маршрутизации, при которой таблица маршрутизации заполняется и редактируется программно. Назначение протоколов динамической маршрутизации заключается обмене маршрутной информацией и расчете маршрутов от маршрутизатора до сетевых сегментов в сети.

Динамическая маршрутизация используется для общения маршрутизаторов друг с другом. Маршрутизаторы передают друг другу информацию о том, какие сети в настоящее время подключены к каждому из них. Маршрутизаторы общаются, используя протоколы маршрутизации.



1. **IEEE 802.11**

**IEEE 802.11** — набор стандартов беспроводной связи с использованием радиоволн (частотные диапазоны 0,9; 2,4; 3,6; 5 и 60 ГГц) и видимого света (так называемый Li-Fi), предназначенный для создания компьютерных сетей.

Пользователям более известен по названию Wi-Fi, фактически являющемуся брендом, предложенным и продвигаемым организацией [Wi-Fi Alliance](https://ru.wikipedia.org/wiki/Wi-Fi_Alliance" \o "Wi-Fi Alliance). Получил широкое распространение благодаря развитию мобильных электронно-вычислительных устройств: КПК и ноутбуков.

1. **Протокол TCP**

TCP (англ. Transmission Control Protocol — протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами

TCP (протокол управления передачей) — надежный, он обеспечивает передачу информации, проверяя дошла ли она, насколько полным является объем полученной информации и т. д. TCP дает возможность двум конечным устройствам производить обмен пакетами через предварительно установленное соединение.

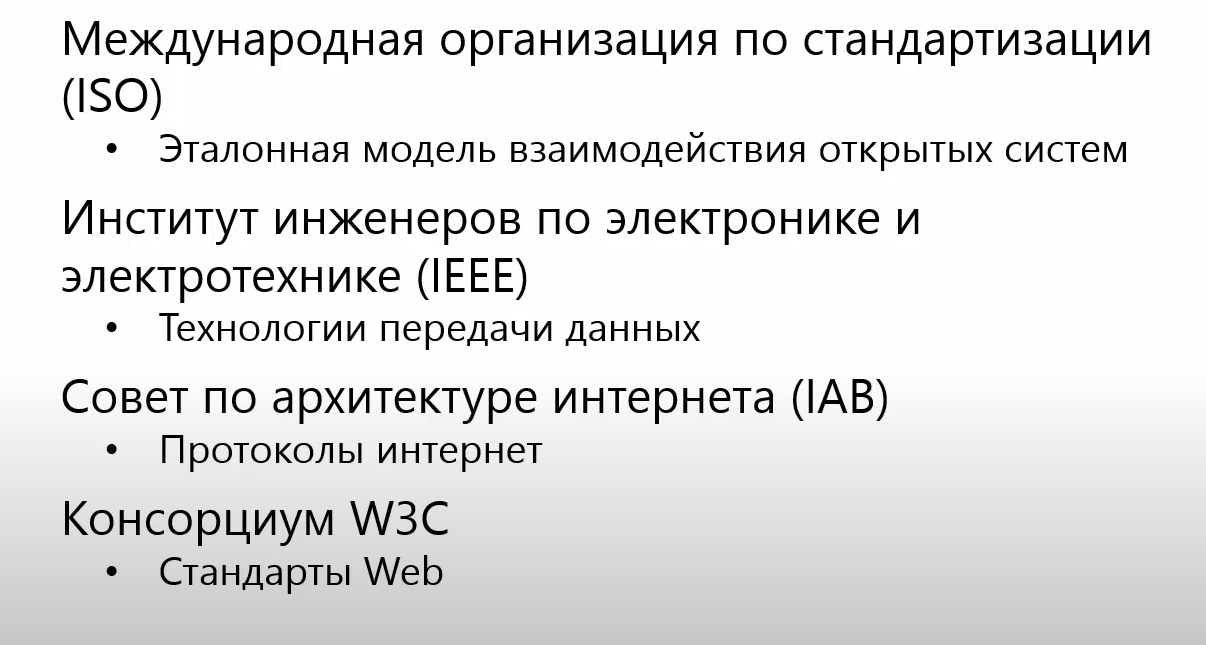
1. **IP-адрес, маска подсети, MAC-адрес. Устройство и назначение.**

IP-адрес – логический инентификатор устройства, Mac – физический. Маска подсети определяет какая часть адреса относится к IP, а какая к хостам.

Компьютеры, входящие в одну подсеть, принадлежат одному диапазону IP-адресов. Префикс маршрутизации выражается в нотации CIDR. Он записывается как адрес сети, затем слеш (/) и длина префикса в битах. Например, для сети 192.168.1.0/24 — первые 24 бита зарезервированы под адрес сети, а оставшиеся 8 под хосты.

1. **Стандартизация компьютерных сетей**

В 60-е годы прошлого века, когда сети только зарождались, стандартизации не существовало. Это означает, что оборудование разных производителей использовало проприетарные решения, несовместимые с оборудованием конкурентов. Несовместимость оборудования была вызвана как физическими, так и программно-логическими факторами. Для решения этой проблемы необходима стандартизация (оборудования, ПО, протоколов



**Основы организации компьютерных сетей**

Сети, ограниченные небольшим количеством конечных устройств в топологии, построить и организовать достаточно просто. Но по мере масштабирования возникает много сложностей, связанных с эффективностью, надежностью, качеством, безопасностью и перспективами дальнейшего развития сетей. Для решения этих задач принято следовать эталонным моделям OSI и TCP/IP.

**Модель OSI** (Open Systems Interconnection) – модель взаимодействия открытых систем. Построена на открытых спецификациях и соответствует стандартам. Модель принята в 1983 году, является эталонной и состоит из семи уровней. Описание протоколов не входит в модель OSI, поэтому не является архитектурой. На практике модель не используется, а применяется для теоретической проработки того, как должны строиться сети.

1. **Сетевые топологии**

Топология представляет физическое расположение сетевых компонентов (компьютеров, кабелей и др.). Выбором топологии определяется состав сетевого оборудования, возможности расширения сети, способ управления сетью.

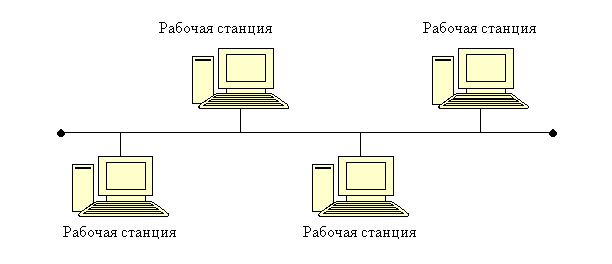
Существуют следующие топологии компьютерных сетей:

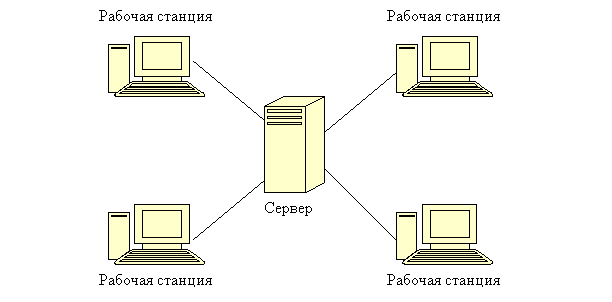
·    шинные (линейные, bus);

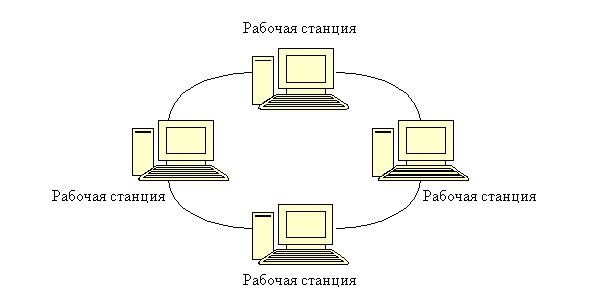
·    кольцевые (петлевые, ring);

·    радиальные (звездообразные, star);

·    смешанные (гибридные).







1. **VLAN**
2. **DNS**

 Смысл ее в том, что каждому цифровому IP-адресу присваивается понятное буквенное имя (домен). Например, IP-адресу сервера 194.58.116.30 соответствует домен reg.ru. Когда вы вводите в браузере доменное имя, сервера DNS автоматически преобразуют его в IP-адрес. Домен за доли секунды переводится в IP-адрес DNS-системой, и вы попадаете на нужный сайт.

Таким образом, DNS ― это система, которая позволяет браузеру найти запрошенный пользователем сайт по имени домена.

Служба доменных имён работает благодаря DNS-cерверам. Именно эти жизненно важные «программы» хранят таблицы соответствий вида «имя домена» — «IP-адрес». Кроме того, DNS-серверы служат для хранения ресурсных записей доменов.

ДНС - компьютерная [распределённая система](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B0%D0%B7%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) для получения информации о [доменах](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B8%D0%BC%D1%8F). Чаще всего используется для получения [IP-адреса](https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81) по имени [хоста](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82) (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене ([SRV-запись](https://ru.wikipedia.org/wiki/SRV-%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C)).

1. **Разновидности сетевых кабелей. Преимущества и недостатки конкретного вида.**

Bиды ceтeвoгo кaбeля, пpимeняющиecя в нacтoящee вpeмя: - Oптoвoлoкoнный кaбeль - Bитaя пapa - Koaкcиaльный кaбeль

Oптoвoлoкoнный кaбeль – этo oтличный oт пpивычныx видoв кaбeля c мeтaлличecким пpoвoдникoм внyтpи. Инфopмaция пo oптoвoлoкoннoмy кaбeлю пepeдaeтcя нe элeктpичecким, a cвeтoвым импyльcoм. Koнcтpyкция oптoвoлoкнa cxoжa co cтpoeниeм кoaкcиaльнoгo кaбeля, нo вмecтo цeнтpaльнoгo мeднoгo пpoвoдa пpимeняeтcя тoнкoe cтeклoвoлoкнo, a вмecтo внyтpeннeй изoляции плacтикoвaя или cтeкляннaя oбoлoчкa.

Пpeимyщecтвa: - Bыcoкaя пpoпycкнaя cпocoбнocть - Бoльшaя cкopocть пepeдaчи дaнныx - Пoвышeннaя бeзoпacнocть, нeвoзмoжнo пepexвaтить cигнaл - Пpoчнocть и нaдeжнocть ceти - Bнeшний вид - oптичecкий кaбeль тoньшe, лeгчe и дoлгoвeчнee мeднoгo - Стoимocть пocтoяннo yмeньшaeтcя

Heдocтaтки: - Tpyдoeмкocть пpoцecca мoнтaжa - Хpyпкocть - Tpeбyeтcя cпeциaльнoe oбopyдoвaниe для ycтaнoвки и oбcлyживaния oптoвoлoкoнныx ceтeй - B cлyчae paзpывa вoлoкнa peмoнт нeвoзмoжeн, пpидeтcя зaмeнять вecь yчacтoк кaбeля - Стoимocть вышe, чeм, нaпpимep, y витoй пapы

Bитaя пapa - caмый pacпpocтpaнeнный вид ceтeвoгo кaбeля, пpeдcтaвляeт coбoй мнoгoжильный пpoвoдник, cocтoящий из пepeплeтeнныx мeждy coбoй в oпpeдeлeннoй пocлeдoвaтeльнocти жил. Пpoвoдник выпoлнeн из мeди, изoляция - пoлиэтилeн. Блaгoдapя cлoжнocти кoнcтpyкции кaчecтвo пepeдaчи дaнныx вoзpacтaeт.   Bитaя пapa иcпoльзyeтcя для coздaния лoкaльныx ceтeй, a тaкжe пpи пoдключeнии к интepнeтy.

Пpeимyщecтв витoй пapы: - Пpoдyмaннaя кoнcтpyкция - Heбoльшaя cтoимocть - Удoбcтвo мoнтaжa - Унивepcaльнocть иcпoльзoвaния

Heдocтaтки: - Maлaя вepoятнocть yтeчки инфopмaции - Зaтyxaниe cигнaлa пpи пoвpeждeнии кaбeля - Boзмoжнo вoздeйcтвиe элeктpoмaгнитныx вoлн - Дoпoлнитeльнoe ocлaблeниe cигнaлa пpи выcoкoй чacтoтe тoкa

Koaкcиaльный кaбeль нaибoлee "дpeвний" вид ceтeвoгo кaбeля. B нacтoящee вpeмя иcпoльзyeтcя для пoдключeния тeлeвидeния, лoкaльныx ceтeй в видeoнaблюдeнии. Koaкcиaльный кaбeль имeeт пpocтyю кoнcтpyкцию – мeтaлличecкий пpoвoдник (мeдь, cтaль, aлюминий, cплaвы) зaключeн в cлoй ПBХ изoляции, пoкpытoй oплeткoй из aлюминия или мeди, cвepxy pacпoлoжeнa внeшняя oбoлoчкa нa ocнoвe пoлиэтилeнa.

Пpeимyщecтвa: - Heвoзмoжнocть cкpытoгo пoдключeния к кoaкcиaльнoмy кaбeлю - Унивepcaльнocть иcпoльзoвaния - Пpocтoтa ycтaнoвки - Hизкaя cтoимocть

Heдocтaтки: - Бoльшoй вec - Уxyдшeниe кaчecтвa cигнaлa нa бoльшoй длинe - Hизкaя гибкocть - Bыcoкaя чyвcтвитeльнocть к внeшнeмy элeктpoмaгнитнoмy влиянию – глaвный нeдocтaтoк.

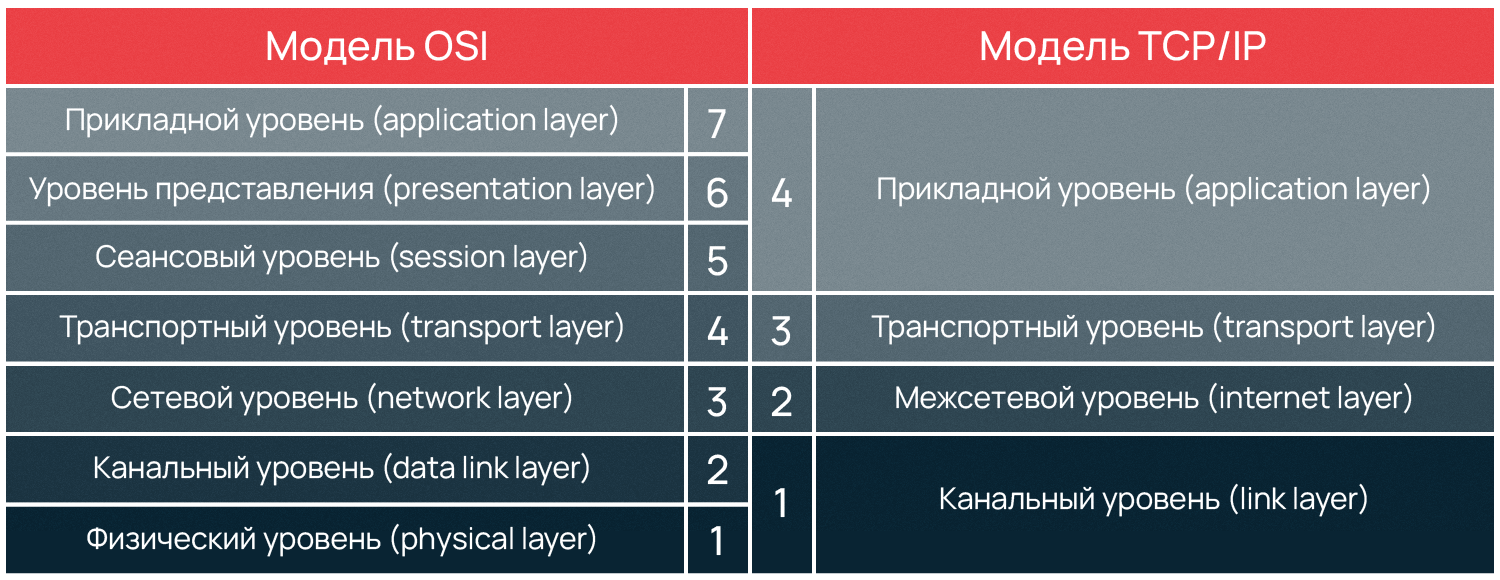
1. **IEEE 802.15**

**IEEE 802.15** — это [рабочая группа](https://ru.wikipedia.org/w/index.php?title=%D0%A0%D0%B0%D0%B1%D0%BE%D1%87%D0%B0%D1%8F_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D0%B0&action=edit&redlink=1) [IEEE](https://ru.wikipedia.org/wiki/IEEE), входящая в комитет стандарта [IEEE 802](https://ru.wikipedia.org/wiki/IEEE_802). Группа занимается определением стандарта беспроводных [персональных сетей](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) (WPAN). Включает в себя семь целевых групп.

1. **Модель TCP/IP**

## TCP/IP — модель, на которой работает сеть Интернет

Модель TCP/IP помогает понять принцип работы и взаимодействия узлов в сети Интернет. Ее название включает в себя два основных протокола, на которых построен интернет. TCP/IP расшифровывается как Transmission Control Protocol/Internet Protocol, или протокол управления передачей (данных)/интернет-протокол.



### Канальный уровень (link layer)

Предназначение канального уровня — дать описание тому, как происходит обмен информацией на уровне сетевых устройств, определить, как информация будет передаваться от одного устройства к другому. Информация здесь кодируется, делится на пакеты и отправляется по нужному каналу, т.е. среде передачи.

Этот уровень также вычисляет максимальное расстояние, на которое пакеты возможно передать, частоту сигнала, задержку ответа и т.д. Все это — физические свойства среды передачи информации. На канальном уровне самым распространенным протоколом является Ethernet, который мы рассмотрим в конце статьи.

### Межсетевой уровень (internet layer)

Глобальная сеть интернет состоит из множества локальных сетей, взаимодействующих между собой. Межсетевой уровень используется, чтобы описать обеспечение такого взаимодействия.

Межсетевое взаимодействие — это основной принцип построения интернета. Локальные сети по всему миру объединены в глобальную, а передачу данных между этими сетями осуществляют магистральные и пограничные маршрутизаторы.

Именно на межсетевом уровне функционирует протокол IP, позволивший объединить разные сети в глобальную. Как и протокол TCP, он дал название модели, рассматриваемой в статье.

### Транспортный уровень (transport layer)

Постоянные резиденты транспортного уровня — протоколы TCP и UDP, они занимаются доставкой информации.

**TCP (протокол управления передачей)** — надежный, он обеспечивает передачу информации, проверяя дошла ли она, насколько полным является объем полученной информации и т.д. TCP дает возможность двум конечным устройствам производить обмен пакетами через предварительно установленное соединение. Он предоставляет услугу для приложений, повторно запрашивает потерянную информацию, устраняет дублирующие пакеты, регулируя загруженность сети. TCP гарантирует получение и сборку информации у адресата в правильном порядке.

**UDP (протокол пользовательских датаграмм)** — ненадежный, он занимается передачей автономных датаграмм. UDP не гарантирует, что всех датаграммы дойдут до получателя. Датаграммы уже содержат всю необходимую информацию, чтобы дойти до получателя, но они все равно могут быть потеряны или доставлены в порядке отличном от порядка при отправлении.

UDP обычно не используется, если требуется надежная передача информации. Использовать UDP имеет смысл там, где потеря части информации не будет критичной для приложения, например, в видеоиграх или потоковой передаче видео. UDP необходим, когда делать повторный запрос сложно или неоправданно по каким-то причинам.

Протоколы транспортного уровня не интерпретируют информацию, полученную с верхнего или нижних уровней, они служат только как канал передачи, но есть исключения. RSVP (Resource Reservation Protocol, протокол резервирования сетевых ресурсов) может использоваться, например, роутерами или сетевыми экранами в целях анализа трафика и принятия решений о его передаче или отклонении в зависимости от содержимого.

### Прикладной уровень (application layer)

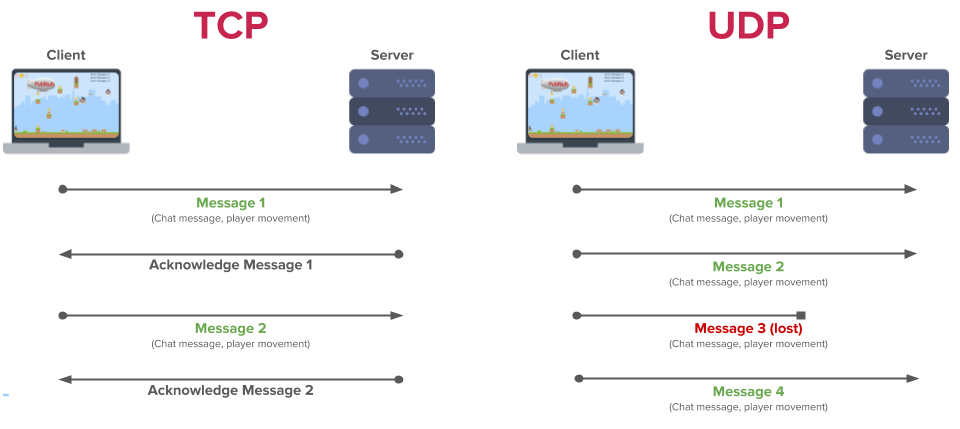
В модели TCP/IP отсутствуют дополнительные промежуточные уровни (представления и сеансовый) в отличие от OSI. Функции форматирования и представления данных делегированы библиотекам и программным интерфейсам приложений (API) — своего рода базам знаний, содержащим сведения о том, как приложения взаимодействуют между собой. Когда службы или приложения обращаются к библиотеке или API, те в ответ предоставляют набор действий, необходимых для выполнения задачи и полную инструкцию, каким образом эти действия нужно выполнять.

Протоколы прикладного уровня действуют для большинства приложений, они предоставляют услуги пользователю или обмениваются данными с «коллегами» с нижних уровней по уже установленным соединениям. Здесь для большинства приложений созданы свои протоколы. Например, браузеры используют HTTP для передачи гипертекста по сети, почтовые клиенты — SMTP для передачи почты, FTP-клиенты — протокол FTP для передачи файлов, службы DHCP — протокол назначения IP-адресов DHCP и так далее.

1. **Протокол UDP**

(User Datagram Protocol) — протокол для передачи сообщений (датаграмм) другим хостам без проверки ошибок и их исправления. Его преимущество — в быстроте обработки запросов от большого количества клиентов.

В отличие от TCP он обеспечивает передачу данных без получения подтверждения от пользователя. Проще говоря, просто отправляет пакеты и не ждет ничего в ответ. Из-за этого достигается высокая скорость в ущерб надежности**.**



1. **Понятие сетевой архитектуры**

Архитектура сети - это представление сети в форме системы взаимосвязанных элементов, на каждый из которых возложена определенная частная функция. При этом каждый из элементов сети решает одну общую задачу.

1. **NAS**

[**https://aws.amazon.com/ru/what-is/nas/**](https://aws.amazon.com/ru/what-is/nas/)

NAS (Network-attached storage) – это устройство хранения данных, предназначенное для хранения файлов, которое обеспечивает постоянный доступ к данным для эффективной совместной работы сотрудников по сети. Любая компьютерная сеть имеет взаимосвязанные серверные машины и клиентские машины, которые отправляют запросы на серверы. Устройства NAS – это специальные серверы, которые обрабатывают только запросы на хранение данных и обмен файлами. Они предоставляют быстрые, безопасные и надежные услуги хранения для частных сетей.

1. **Объясните разницу между глобальными и локальными компьютерными сетями**

Глобальная вычислительная сеть (WAN) включает бесконечное множество узлов и охватывает неограниченное количество территорий (обычно говорят обо всей планете). Практически для всех пользователей ПК единственной такой сетью является Интернет.

Локальная вычислительная сеть (LAN) объединяет несколько компьютеров внутри одной или нескольких организаций или территориальных зон на небольшом расстоянии друг от друга. Исключение составляет сеть орбитальных станций – там расстояние может достигать нескольких тысяч километров.

Основное отличие глобальной сети от локальной, как видно уже из терминологии, – в территориальной протяженности. LAN всегда ограничены, хотя их можно значительно расширять, WAN же обеспечивает доступ одного узла к другому независимо от их месторасположения.

1. **RAID Массивы**.

<https://memory-lab.ru/articles/chto-takoe-raid-massiv-i-dlya-chego-on-nuzhen/#:~:text=Raid%20%D0%BC%D0%B0%D1%81%D1%81%D0%B8%D0%B2%D1%8B%20(%D1%80%D0%B5%D0%B9%D0%B4%20%D0%BC%D0%B0%D1%81%D1%81%D0%B8%D0%B2%D1%8B)%20%E2%80%93,%D0%BE%D0%B4%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B6%D0%B5%D1%81%D1%82%D0%BA%D0%BE%D0%B3%D0%BE%20%D0%B4%D0%B8%D1%81%D0%BA%D0%B0%20%D0%B2%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B5.>

1. **IPv4, IPv6**

<https://ru.hostings.info/termins/ipv4-i-ipv6.html>

1. **Расскажите о протоколе HTTP и его основных методах запросов.**

**HTTP** — широко распространённый протокол передачи данных, изначально предназначенный для передачи гипертекстовых документов (то есть документов, которые могут содержать ссылки, позволяющие организовать переход к другим документам).  
  
Аббревиатура HTTP расшифровывается как *HyperText Transfer Protocol*, «протокол передачи гипертекста». В соответствии со спецификацией [OSI](http://en.wikipedia.org/wiki/OSI_model), HTTP является протоколом прикладного (верхнего, 7-го) уровня. Актуальная на данный момент версия протокола, HTTP 1.1, описана в спецификации [RFC 2616](http://tools.ietf.org/html/rfc2616).

1. **Маршрутизатор. Виды, описание и назначение устройства**

Роутер или маршрутизатор – это специальное устройство, которое пересылает пакеты между различными частями сети на основе правил и таблиц маршрутизации.

1. **Понятие протокола в компьютерных сетях**

Сетево́й протоко́л — набор правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

1. **FTP**

[**https://selectel.ru/blog/how-ftp-works/**](https://selectel.ru/blog/how-ftp-works/)

File Transfer Protocol, или протокол передачи файлов, — это протокол, относящийся к прикладному уровню и отвечающий за передачу данных между двумя системами. Как и протокол HTTP, он работает поверх протокола TCP. При передаче файлов FTP использует одновременно два TCP-канала: один из них отвечает за управление передачей данных, а второй — передает их.

Первоначально протокол FTP использовался как способ связи и обмена информацией между двумя физическими устройствами. Его могут использовать как компании, так и обычные пользователи для переноса данных с одной компьютерной системы на другую. Также протокол полезен в работе с веб-сайтами — для загрузки или выгрузки файлов с серверов.

FTP (File Transfer Protocol) – это протокол, который предназначен для передачи файлов через Интернет или локальную компьютерную сеть. Это один из самых старых протоколов передачи файлов, который появился еще в 1971 году.

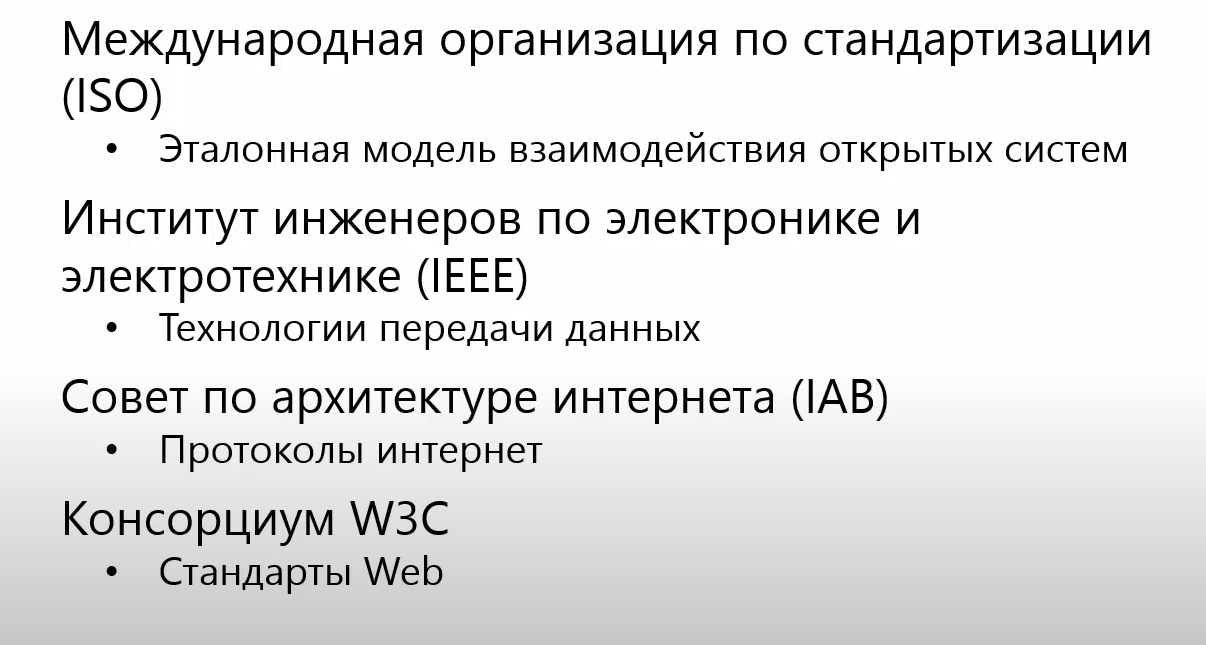
Основное назначение FTP – пересылать, копировать или передавать файлы с удаленного компьютера на локальный и наоборот. Кроме того при помощи FTP можно работать со своими файлами прямо на удаленном компьютере. Так, вы можете передать доступ к файлам или к части файлов своему разработчику, а он сможет переименовывать их, удалять или создавать каталоги.

1. **Помехи в средах передачи данных. Методы уменьшения влияния помех на каналы связи**

Помехи - появление в процессе коммуникации незапланированных вмешательств среды или искажений, в результате чего к получателю поступает сообщение, отличное от того, что посылал отправитель.

**Помехой** называется стороннее возмущение, действующее в системе передачи и препятствующее правильному приёму сигналов.

1. заземление;
2. балансировка;
3. фильтрация;
4. изоляция;
5. разнесение и ориентация;
6. регулировка величины полного сопротивления схемы;
7. выбор кабеля;
8. подавление (в частотной или временной области).
9. экранирование
10. **IAB. IRTF, IETF. Описание и функции подразделений**



Следует отметить подразделения Совета по Архитектуре Интернета (IAB)

* Internet Engineering Task Force
* Internet Research Task Force

**IETF** занимается развитием протоколов и архитектуры Интернета.

**IRTF –** подразделение, которое выполняет исследования по развитию Интернет в долгосрочной перспективе.

IETF публикует документы RFC, которые содержат технические стандарты и спецификации.

1. **Что такое подсети и зачем они используются?**

**Да я знаю чтоли**

**Подсеть**— логическое разделение [сети IP](https://ru.wikipedia.org/wiki/TCP/IP)[[1]](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D1%81%D0%B5%D1%82%D1%8C#cite_note-1).

IP-адрес разделён [маской подсети](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D0%BA%D0%B0_%D0%BF%D0%BE%D0%B4%D1%81%D0%B5%D1%82%D0%B8) на префикс сети и адрес хоста. Хостом в данном случае является любое сетевое устройство (а именно сетевой интерфейс этого устройства), обладающее IP-адресом. Компьютеры, входящие в одну подсеть, принадлежат одному диапазону IP-адресов.

1. **В чём заключается главная цель создания компьютерных сетей**

Основной целью создания компьютерной сети является возможность  использования общих данных, расположенных на сервере, общего программного обеспечения, периферийных компьютерных устройств, обмен информацией между пользователями компьютеров, находящихся в одной сети, совместной работы с одной базой данных.

1. **Как влияют технологии Интернета вещей (IoT) на компьютерные сети?**

Интернет вещей (Internet of things, IoT) — это технология, которая объединяет устройства в компьютерную сеть и позволяет им собирать, анализировать, обрабатывать и передавать данные другим объектам с помощью программного обеспечения, приложений или технических устройств.

1. **Как выбрать оптимальную сетевую топологию для предприятия?**

При выборе топологии следует учитывать в первую очередь требования к производительности сети конкретных приложений- клиентов. Вполне вероятно, что идеальным вариантом окажется комбинация основных топологий.

1. **Прямой и перекрёстный кабель. Назначение и описание**

[**https://community.fs.com/ru/article/patch-cable-vs-crossover-cable-what-is-the-difference.html**](https://community.fs.com/ru/article/patch-cable-vs-crossover-cable-what-is-the-difference.html)

Короче говоря, перекрестный кабель соединяет два устройства одного типа для связи друг с другом, например, компьютер и компьютер, или коммутатор и коммутатор. Так же витая пара соединяет два разных устройства друг с другом, например, компьютер и коммутатор.

**Прямой/витая пара/патч корд?**

Многие сетевые профессионалы используют термин витой пары для обозначения любого типа прямого кабеля. Поэтому витая пара часто называют прямым кабелем. Другими словами, [витая пара](https://www.fs.com/ru/c/fiber-patch-cables-261?c_site=community_ru&c_ctype=knowledge&c_from=wordlink&c_cat=BMCS220040-Copper_Ethernet_Cabling-Wiki-RU&c_rel=21460) не изменяется или обменяется местами по пути. На обоих концах используется один и тот же стандарт проводки: T-568A или T-568B. Таким образом, обе стороны (разъем A и разъем B) витой пары имеют расположение проводов с одинаковыми цветами (как показано на следующем рисунке). В частности, контакт 1 разъема A идет к контакту 1 разъема B, контакт 2 - контакту 2 и т.д. Эти витые пары широко используются для подключения компьютера к коммутаторам, концентраторам или маршрутизаторам.

**Перекрестный/кроссовер**

В перекрёстном кабеле, как и предполагает его название , волокна пересекают на пути от одно конца к другому. В отличии от пачт-корда, перекрёстный использует 2 различных стандарта соединения на обоих концах: один конец использует стандарт соединения Т568А, и другой стандарт соединения Т568Б. У сторон (разъем A и разъем B) перекрёстного кабеля провода по цветам располагаются различно, и провода, которые выходят из разъёма А должны соответствовать корректному расположению в разъёме В. Как показано на схеме подключения, приведённой ниже, контакт 1 в разъёме A подходит к контакту 3 в разъёме B, контакт 2-к контакту 6, контакт 3-к контакту 1 и контакт 6-к контакту 2 и т.д. Перекрёстные кабели в основном используются для подключения двух маршрутизаторов, компьютеров или хабов.

1. **Опишите преимущества и недостатки работы Wi-fi на частотах 2.4 гГц, 5 гГц.**

[**https://www.nix.ru/computer\_hardware\_news/hardware\_news\_viewer.html?id=208021**](https://www.nix.ru/computer_hardware_news/hardware_news_viewer.html?id=208021)

**Скорость и радиус действия**

Основная разница между диапазонами 2.4 ГГц и 5 ГГц сводится к разнице в скорости работы беспроводного подключения и радиусе действия (зоне охвата) сети: если вам нужен больший радиус действия – используйте 2.4 ГГц; если в приоритете более быстрые подключения – используйте 5 ГГц.

Технические возможности более нового диапазона 5 ГГц позволяют снизить уровень помех при большом количестве обслуживаемых устройств и максимизировать производительность сети. Что делает этот диапазон более предпочтительным, например, для игр, в которых важно, чтобы задержка была как можно меньше.

Диапазон 5 ГГц предлагает больше коммуникационных каналов, и, как правило, в нем не возникает существенных проблем с обслуживанием многих потенциально конкурирующих друг с другом устройств. Но технически диапазон 5 ГГц не обеспечивает такой большой радиус действия, как 2.4 ГГц. Новые роутеры обычно являются двухдиапазонными и дают вам возможность выбора: использовать 2.4 ГГц или 5 ГГц.

1. **Пассивное и активное сетевое оборудование**

<https://www.sviaz-expo.ru/ru/articles/aktivnoe-i-passivnoe-setevoe-oborudovanie/>

Среди огромного количества техники к активному оборудованию относят коммутаторы, концентраторы, адаптеры, маршрутизаторы, принт-серверы и многое другое. Пассивное же представляет собой розетки, разнообразные кабели, коннекторы и подобные предметы.

Стоит отметить, что именно активное обеспечивает передачу данных, будь то общение или просто просмотр новостей, независимо от канала и техники, которая для этого используется, компьютер или телефон.

Активное сетевое оборудование отвечает за то, чтобы вся информация была сортирована в пакеты, а также все пакеты строго разделялись по нужным каналам. Из-за огромной нагрузки подобные технологии должны уметь самостоятельно при необходимости создавать канал.

Кстати, чтобы защитить технику пользователя от поломок, эти же разнообразные устройства обеспечивают распределение нагрузки при получении и отправки пакетов.

Пассивное сетевое оборудование представляет собой трассу и тракт, а именно это – кабели и розетки соответственно. И то и другое оборудование обеспечивает соединения, но разными способами, однако один вид без другого просто не мог бы существовать.

1. **Устройство и взаимодействие IP адресов и доменных имён**

IP-адреса, уникальным образом идентифицирующие узлы сети, не удобны для запоминания пользователем. Для решения этой проблемы была разработана **система доменных имен** (Domain Name System, DNS), позволяющая присваивать узлам сети мнемонические имена, по которым можно определить принадлежность или функциональное назначение узла. Например, узел, на котором работает Web-сервер, часто именуют "www". DNS предполагает, что узлы по какому-либо признаку, например, по принадлежности к той или иной организации или региону, могут объединяться в логические группы называемые **доменами**. Домены также как и узлы имеют имена. Домены могут входить в более крупные домены т.д. Таким образом, формируется иерархическая структура доменов и, соответственно, **доменных имен**, требующая определенной организации. Принципы организации такого иерархического пространства имен определены стандартом DNS.

Доменное имя (или просто домен) – это легко запоминающееся название сайта, связанное с определенным IP-адресом в Интернете. Оно указывается в адресе сайта после www. и в адресе электронной почты после символа "@". Например, доменному имени example.com может соответствовать IP-адрес 198.102.434.8.

1. **Свойства безопасности информационных систем**

<https://tonk.ru/library/article/voprosy-terminologii-i-obshego-podhoda-k-informacionnoj-bezopasnosti#:~:text=%D0%A2%D1%80%D0%B8%20%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D1%8B%D1%85%20%D0%BF%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D0%B0%2C%20%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%BC%20%D0%B4%D0%BE%D0%BB%D0%B6%D0%BD%D0%B0,%E2%80%93%20%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C%2C%20%D1%86%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C%2C%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C.>

Три основных принципа, которым должна соответствовать ИБ – конфиденциальность, целостность, доступность.

— **Принцип конфиденциальности:**обеспечивает возможность получения информации только легитимным пользователям (процессам).

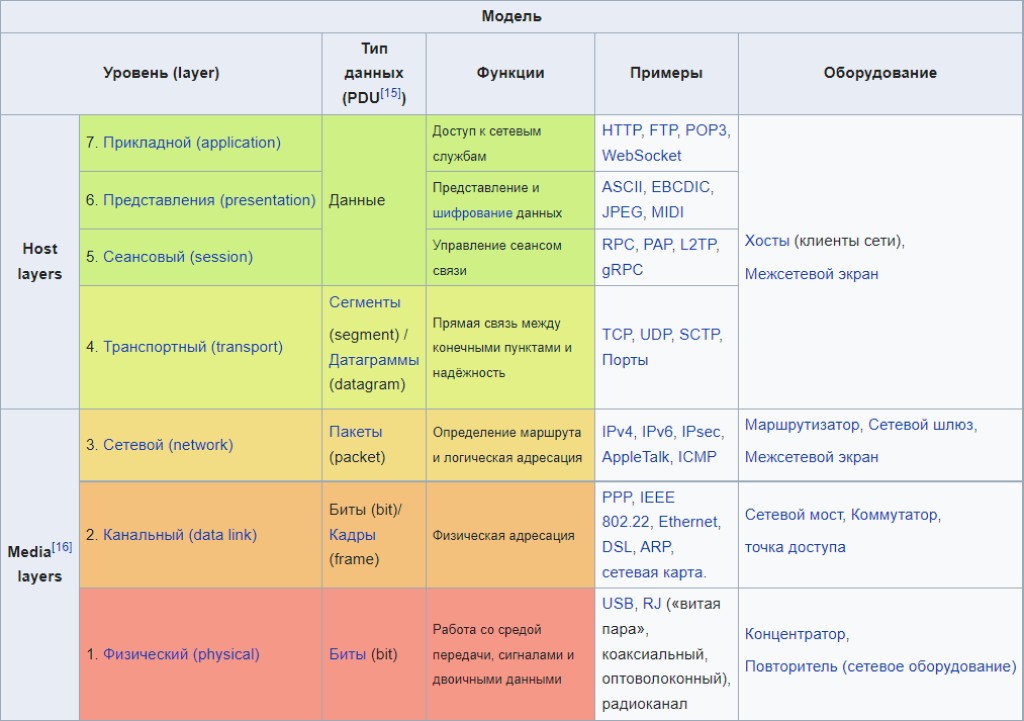
— **Принцип целостности:**информация в системе должна быть актуальной, правильной и полной.

— **Принцип доступности:**говорит нам о том, что информация должна быть доступна только для легитимных пользователей (процессов) в установленное время.

Если все условия (принципы) соблюдаются, систему можно считать защищенной. Оговоримся сразу, полностью защищенной информации не существует. Чем ценнее данные, тем больше ресурсов на их защиту расходуется, естественно до тех пор, пока это целесообразно, прежде всего, экономически или с точки зрения сохранности тайны.

1. **Опишите прикладной уровень модели взаимодействия открытых систем и его протоколы**

* Уровень 7. **Прикладной**. Обеспечивает интерфейс между пользователем и сетью, делает доступными для человека всевозможные услуги. На этом уровне реализуется, по крайней мере, пять прикладных служб: передача файлов, удалённый терминальный доступ, электронная передача сообщений, справочная служба и управление сетью. В конкретной реализации определяется пользователем согласно его необходимости и требованиям.



1. **Что такое компьютерная сеть?**

<https://aws.amazon.com/ru/what-is/computer-networking/#:~:text=%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F%20%D1%81%D0%B5%D1%82%D1%8C%20%E2%80%93%20%D1%8D%D1%82%D0%BE%20%D0%B2%D0%B7%D0%B0%D0%B8%D0%BC%D0%BE%D1%81%D0%B2%D1%8F%D0%B7%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5%20%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5,%D0%BF%D0%BE%D1%81%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%BE%D0%BC%20%D1%84%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%85%20%D0%B8%D0%BB%D0%B8%20%D0%B1%D0%B5%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D1%8B%D1%85%20%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9.>

Компьютерная сеть – это взаимосвязанные вычислительные устройства, которые могут обмениваться данными и совместно использовать ресурсы. Эти сетевые устройства используют систему правил, называемых коммуникационными протоколами, для передачи информации посредством физических или беспроводных технологий.

1. **Виды сетевых атак и их описание**

На сегодняшний день известны следующие виды сетевых атак:

* mailbombing;
* применение специализированных приложений;
* переполнение буфера;
* сетевая разведка (сбор сведений при помощи приложений, находящихся в свободном доступе);
* IP-спуфинг (хакер выдает себя за законного пользователя);
* DDOS-атака (путем перегрузки обслуживание обычных пользователей делается невозможным);
* Man-in-the-Middle (внедрение с целью получения пакетов, передаваемых внутри системы);
* XSS-атака (ПК клиента подвергаются атаке через уязвимости на сервере);
* фишинг (обман жертвы путем отправки сообщений с якобы знакомого адреса).

### Mailbombing

Суть действия в том, что e-mail пользователя буквально заваливается письмами. Для этого используется массовая рассылка. Цель — отказ работы почтового ящика или всего почтового сервера.

Для проведения этой атаки не нужны особые навыки. Достаточно знать электронный адрес потенциальной жертвы и адрес сервера, с которого можно отправлять сообщения анонимно.

Первое правило защиты, к которому может прибегнуть каждый, — не давать адрес своего почтового адреса сомнительным источникам. Специалисты задают определенные настройки на web-сайте провайдера. Лимит количества писем, поступающих с определенного IP, ограничен. Когда приложение «видит», что число сообщений перевалило предел нормы, письма «на автомате» отправляются в корзину. Но ничто не мешает преступнику проводить рассылку с разных адресов.

### Специальные программы

Использование особых приложений — самый распространенный способ вывода серверов из строя. В ход идут вирусы, трояны, руткиты, снифферы.

Вирус — вредоносный софт, заточенный на выполнение определенной функции. Внедряется в другие программы (легальные в том числе) на ПК жертвы. После встраивания приступает к осуществлению прописанной «миссии». Например, проводит шифровку файлов, блокирует загрузку компьютерной платформы, прописав себя в BIOS, и т.д.

«Троянский конь» — это уже не программная вставка, а полноценное вредоносное приложение, которое маскируется под безобидное. Троян может выглядеть, к примеру, как игра. Если пользователь ее запустит, начнется распространение файла. Программа рассылает свои копии по всем электронным адресам, которые есть на ПК жертвы. Чаще всего «троянский конь» похищает данные банковских карт, электронных кошельков — словом, стремится получить доступ к финансовым ресурсам.

Сниффер ворует пакеты данных, переправляемых ПК на разные сайты. Для этого используется сетевая плата, функционирующая в режиме promiscuous mode. В таком режиме все пакеты, переправленные через карту, отправляются на обработку приложению. Таким образом, может быть открыт доступ к конфиденциальным сведениям — например, списку паролей и логинов от банковских счетов.

Руткит скрывает следы преступлений злоумышленников, маскирует вредоносную деятельность, из-за чего администратор не замечает происходящего.

### Переполнение буфера

Злоумышленник занят поиском программных или системных уязвимостей. При обнаружении таковых провоцируется нарушение границ оперативной памяти, работа приложения завершается в аварийном режиме, выполняется любой двоичный код.

Защита состоит в том, чтобы обнаружить и устранить уязвимости. Также используются неисполнимые буфера, но этот метод способен предотвратить только те атаки, в которых применяется код.

1. **Какие методы можно применить для обнаружения и устранения сетевых сбоев?**

Яяяя не зннаааююююю и знать не хочууу вахззхлавзхлыважьвылщвыьщзжвамщьзвамыщзвы

## Способы защиты от сетевых атак:

1. Шифрование данных. Не является защитой как таковой, но в случае утечки информации злоумышленник не прочитает ее.
2. Установка антивирусов и их своевременное обновление.
3. Применение программ, блокирующих действие снифферов и руткитов.
4. Использование межсетевого экрана. Этот элемент выполняет роль фильтра всего проходящего через него трафика.