

**Адресация в Интернете. Протоколы. Протокол передачи данных TCP/IP.
Доменная система имен. Службы Интернет. Защита информации в Интернете.**

Цели занятия

Образовательные:

- ввести представление о IP-адресе компьютера и системе доменных имен;
- изучить возможности поиска и опознания компьютера в Интернете при помощи IP-адреса и доменного имени;
- первичное закрепление полученных знаний.

Воспитательные:

- Повышение положительной мотивации обучающихся в изучении информатики;
- Активизация познавательной деятельности;
- Воспитание аккуратности, добросовестности.

Развивающие:

- Формирование умений анализировать, выделять главное.

Тип занятия: комбинированный урок.

Формы работы обучающихся: в парах, индивидуальная,

Необходимое техническое оборудование: мультимедийный проектор, персональные компьютеры для обучающихся.

Группа: 28-ДО

Предмет: Информатика

План занятия:

1. Организационный момент (1-2 минуты).
2. Проверка домашнего задания (1-2 минуты).
3. Актуализация знаний (5 минут).
4. Объяснение нового материала (20 минут).
5. Работа за компьютерами (5 минут).
6. Домашнее задание (1 минута).
7. Подведение итогов (2-5 минут)

Учебник:

Ход занятия

Слайд 1.

1. Организационный момент: приветствие обучающихся, проверка отсутствующих.
«Доброе утро! Улыбнитесь своему соседу, улыбнитесь мне. Всё, к занятию готовы».

Девиз занятия: «Я слышу и забываю. Я вижу и запоминаю. Я делаю и понимаю»
(Конфуций)

Слайд 2.

2. Проверка домашнего задания. Фронтальный опрос:

1. Что такое компьютерная сеть?

Ответы обучающихся: Компьютерная сеть — это совокупность компьютеров, объединенных каналами связи, по которым осуществляется прием и передача информации.

2. Назовите основные виды компьютерных сетей.

Ответы обучающихся: локальная сеть и глобальная сеть

Слайд 3

1. Какие сети называют локальными?

Ответы обучающихся: Локальная сеть — это объединение компьютеров, расположенных на небольшом расстоянии друг от друга.

2. Какие сети называют глобальными?

Ответы обучающихся: Глобальная сеть — это объединение компьютеров, расположенных на большом расстоянии, для общего использования мировых информационных ресурсов.

Слайд 4.

Способы поиска информации в интернет?

Ответы обучающихся:

а) указание адреса страницы

б) передвижение по гиперссылкам

в) обращение к поисковому серверу

Что такое электронная почта?

Ответы обучающихся: Электронная почта — это система пересылки электронной корреспонденции между пользователями телекоммуникационной сети.

Слайд 5

Что такое Интернет.

Ответы обучающихся: всемирная глобальная компьютерная сеть

3. Актуализация знаний на основе ранее изученного материала. (Слайд 6)

Преподаватель: Вы знаете что Интернет — это всемирная система объединенных сетей. По итогам статистики, к концу 2020 года число пользователей, регулярно использующих Интернет, составило около 4,2 млрд человек.

Слайд 7.

Интернет состоит из многих тысяч корпоративных, научных, правительственных и домашних компьютерных сетей.

Как вы думаете, как компьютеры находят друг друга в сети, ведь все сайты, которые мы посещаем находятся на разных компьютерах и достаточно удаленных друг от друга?

Ответы обучающихся: Компьютеры находят друг друга по уникальным номерам.

- Что необходимо знать отправителю и получателю для правильной доставки информации с одного компьютера на другой? (адрес компьютера в сети Интернет)

- Каждый компьютер, подключенный к сети Интернет должен иметь свой собственный уникальный адрес? (да)

- Встречали ли вы где-нибудь такой адрес? (да, на своем компьютере дома)

- А как он выглядит? (набор цифр, разделенных точками)

В компьютерах вся информация представляется в цифровом виде, поэтому адрес, который используют компьютеры, является цифровым.

4. Объяснение нового материала.

Слайд 8. Тема представлена на доске, запишите ее в тетради.

Адресация в интернете

Адресация в интернете — это процедура присваивания разным устройствам уникальных адресов для определения маршрута передачи данных.

Основной элемент адресации — IP-адрес.

Кроме IP-адресов, в интернете используются и другие виды адресации, например:

- **MAC-адрес.** Это номер, который присваивается сетевому интерфейсу оборудования. У компьютеров может быть несколько таких интерфейсов, и каждый из них имеет собственный адрес-идентификатор.
- **URL.** Это уникальное имя сайта или сервиса в пределах глобальной сети.
- **Доменный адрес.** Домен — это имя, которое служит для перевода других имён, назначенных для устройства, в IP-адрес.

Для связи IP-адреса и доменного имени на специальных серверах (DNS-серверы) хранятся таблицы, состоящие из пар «IP-адрес и доменное имя».

Каждый компьютер подключенный к сети Интернет должен иметь собственный адрес: IP адрес (Internet Protocol). Именно об этих адресах и вообще об адресации в сети интернет и пойдет речь на этом занятии.

Протоколы

Протокол передачи данных простыми словами — это правила «общения» между компьютерами или устройствами. Он определяет, как данные упаковываются, отправляются и как устройства должны взаимодействовать друг с другом.

Например, когда пользователь вводит в поисковой системе веб-адрес и нажимает Enter, браузер использует протокол HTTP (Hypertext Transfer Protocol), чтобы отправить запрос на сервер.

Сервер отвечает, и браузер интерпретирует полученные данные, чтобы отобразить веб-страницу.

Здесь HTTP — это протокол, который регулирует обмен данными между компьютером и сервером.

Протоколы поддерживают единообразие и определённые стандарты.

Некоторые протоколы с помощью шифрования гарантируют надёжность и безопасность передачи данных, контролируют ошибки.

Протокол передачи данных TCP/IP

Слайд 9.

Узнаем о главной «курьерской службе» интернета: как данные летают по Сети, зачем их фасуют по пакетам и кто за всем этим следит.

Вы когда-нибудь задумывались, как мемы, сериалы и гифки с котиками перелетают континенты, чтобы оказаться у вас на компьютере? Ответаем: для этого в интернете есть протоколы TCP и IP — они помогают устройствам безошибочно передавать данные на большие расстояния. Как у них это получается — узнаем в лекции.

TCP/IP — это общее стандартное название двух протоколов, TCP и IP. Вместе они образуют универсальный стек протоколов передачи данных.

TCP (Transmission Control Protocol) отвечает за обмен данными. Он управляет их отправкой и следит за тем, чтобы они дошли до получателя в целостности.

IP-адрес (*айпи-адрес*, сокращение от англ. *Internet Protocol Address*) — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. Отвечает за адресацию. Его задача — связывать друг с другом устройства и нарезать данные на пакеты для удобной отправки. Чтобы протокол мог быстро найти дорогу от одного компьютера к другому, используются IP-адреса — уникальные идентификаторы, которые есть у каждого устройства в Сети.

Эти два протокола работают в связке: IP строит маршрут, а TCP контролирует, чтобы всё передавалось правильно. Условно их можно сравнить с тандемом Шерлока и Ватсона в бессмертной классике Дойля: первый решает проблему, а второй следит, чтобы тот не наделал глупостей и случайно не упал в Рейхенбахский водопад.

Минутка истории. Оба протокола, и TCP, и IP, на самом деле стары как мир. Их придумала ещё в семидесятых группа разработчиков под началом «отца интернета» Винта

Сёрфа. То есть все наши смартфоны и умные часы общаются по правилам, которые заложили ещё во времена расцвета диско и космической миссии «Союз — Аполлон».

Но протоколами TCP и IP модель не ограничивается — например, есть ещё HTTP, FTP, UDP и сотни других. Все они заточены под определённые задачи. Так, HTTP помогает браузеру формировать запросы к серверу, FTP — скачивать файлы, а UDP — быстро передавать видео, музыку и игры, но с возможными потерями по пути.

Как работает TCP/IP

Настало время посмотреть, как модель TCP/IP работает в жизни. Допустим, вы заходите в интернет, чтобы почитать статью о том, как нейросети рисуют котиков. Запускаете браузер, открываете сайт Skillbox Media, нажимаете на заголовок статьи. А дальше начинается магия.

Как только вы кликнули на ссылку, браузер отправляет запрос на сервер, где лежит страница. Для этого он создаёт HTTP-запрос, в котором описывает всё, что сервер должен ему передать: «Я слышал, у тебя есть статья про генеративные нейронки. Дай, пожалуйста». Сервер отвечает: «Нет проблем» — и отправляет браузеру HTTP-ответ с нужными данными. И так они будут общаться до тех пор, пока вы не закроете сайт.

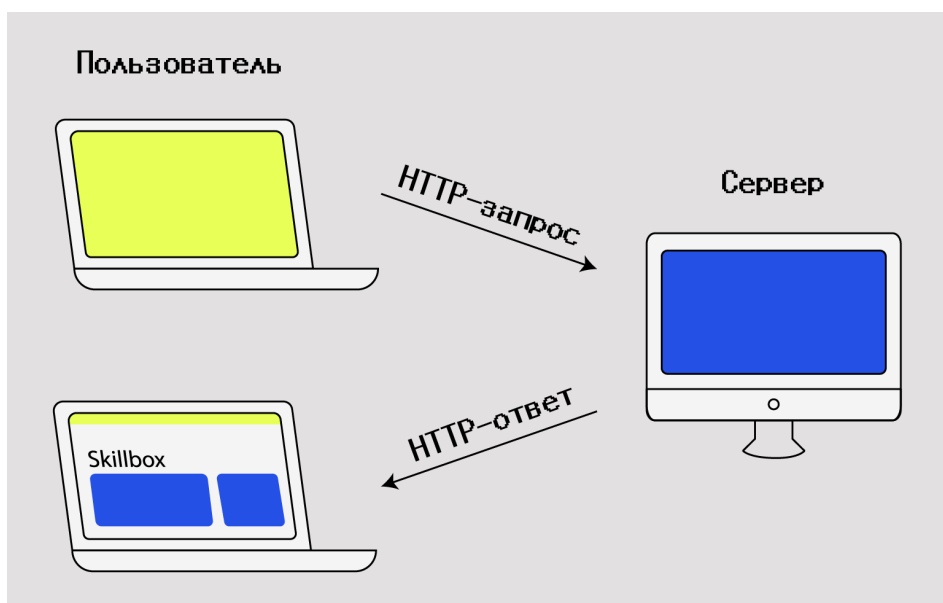


Рисунок 1. Браузер отправляет запрос, сервер возвращает ответ

Но сами по себе HTTP-запросы — это просто текстовые сообщения: они не знают, как найти сервер с нужной информацией, а тем более — как её оттуда достать. Для этих задач нам как раз и понадобятся протоколы TCP и IP.

Сначала IP определяет расположение сервера — или, точнее сказать, его IP-адрес. Чтобы найти нужный «айпишник», протокол использует систему DNS. Это такая глобальная база данных, где доменные имена сайтов лежат напротив их IP-адресов — например, сайту skillbox.ru соответствует IP-адрес 178.248.237.96.

Когда IP найдёт сервер и получит от него нужную страницу, он начнёт разбивать её на пакеты. Каждый пакет — это часть файла размером от 1 до 64 КБ. Внутри находятся сами данные и служебная информация: номер пакета, адреса отправителя и получателя и другое.

Зачем нужны пакеты. Представьте, что вам нужно перенести сразу много блюд из кухни в гостиную. Конечно, можно загрузить тарелки в обе руки, а часть поставить на голову, как делают женщины кенийского племени Луо, но, если вдруг в коридоре на вас нападёт кошка или младший брат с игрушечным пистолетом, есть риск всё выронить и испортить ужин. Гораздо безопаснее переносить блюда по одному, а ещё лучше — раздать по тарелке каждому члену семьи.

С данными точно так же: лучше передавать их маленькими порциями, так как никогда не знаешь, где по пути случится проблема. Если что-то пойдёт не так, вы потеряете всего один пакет, а не весь файл целиком.

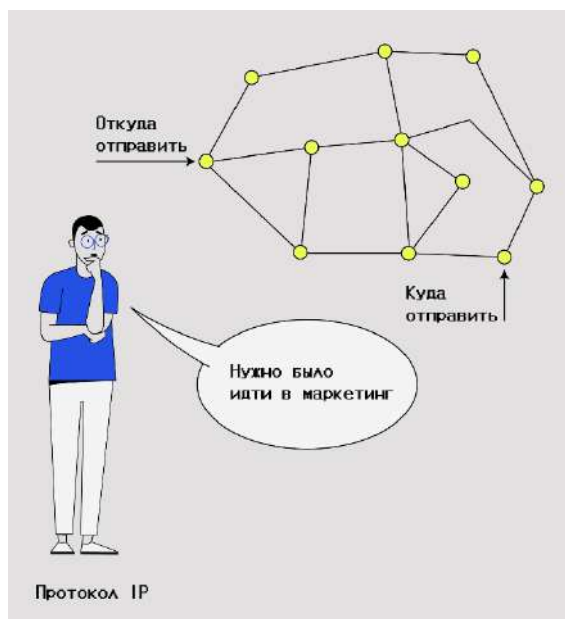


Рисунок 2. Протокол IP ищет нужный путь, советуясь с системой DNS.

Чтобы пакеты без потерь долетали от сервера к пользователю, подключается протокол TCP. Для этого в него зашили механизм подтверждения: когда сервер отправляет пакет, TCP спрашивает у устройства пользователя, нормально ли он добрался. Если ответ «да», протокол отправляет следующую порцию, если «нет» — пробует ещё раз.

После того как все пакеты получены, браузер собирает из них цельную страницу и выводит на экран.

Повторим ещё раз весь процесс:

Вы нажимаете на ссылку или вводите адрес сайта в строке браузера.

Браузер создаёт HTTP-запрос к серверу, чтобы тот отправил вам нужную страницу.

Протокол IP с помощью системы DNS находит сервер, где лежит страница, и разбивает её на пакеты.

Далее в игру вступает TCP — он устанавливает надёжное соединение между компьютером и сервером и следит, чтобы пакеты не потерялись по дороге.

Браузер склеивает пакеты воедино и рендерит страницу.

Этот алгоритм справедлив для статичных файлов — то есть таких, которые вы загружаете один раз и пользуетесь. Но если вы, например, хотите посмотреть видео, понадобится другой протокол — UDP. Он не гарантирует целостности данных и может потерять пакеты по пути, но это компенсируется скоростью передачи. Именно поэтому, например, вы видите пиксельные изображения, когда смотрите видео при плохом интернет-соединении.

Из каких уровней состоит TCP/IP

Пора окунуться в детали и узнать, как модель TCP/IP устроена изнутри. Глобально она делится на четыре уровня:

канальный уровень — отвечает за взаимодействие по сетевому оборудованию, например по Ethernet-кабелю или Wi-Fi;

межсетевой уровень — помогает отдельным сетям общаться друг с другом;

транспортный уровень — отвечает за передачу данных между устройствами, например, по протоколам TCP и UDP;

прикладной уровень — помогает приложениям общаться друг с другом с помощью интерфейсов или API.



Рисунок 3. Структура модели TCP/IP

На каждом уровне есть свои протоколы, которые обеспечивают надёжность передачи данных между компьютерами в Сети. Всего модель TCP/IP поддерживает сотни разных протоколов.

Канальный уровень

Для чего нужен: устанавливать физическое соединение между устройствами в локальной сети с помощью радиоволн и проводов.

Примеры протоколов: Ethernet, Wi-Fi, Bluetooth.

Как работает: данные делятся на небольшие кусочки (фреймы) и передаются между устройствами. Каждый фрейм содержит часть передаваемой информации и служебные данные.

Чтобы понять, куда отправлять фреймы, используют адресацию канального уровня — MAC-адреса. Это уникальные физические адреса устройств — по ним протоколы канального уровня определяют отправителей и получателей.

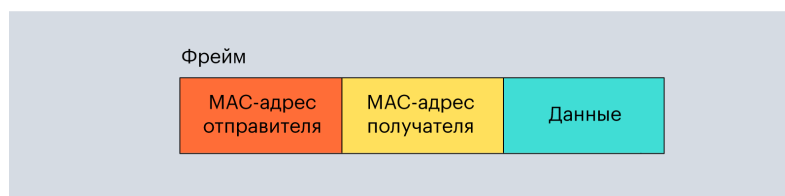


Рисунок 4. Из чего состоит фрейм.

Ещё одна важная задача канального уровня — проверять, что данные передаются безошибочно. Для этого протоколы используют свои средства проверки:

Если возникла ошибка, устройство отправляет фрейм обратно, а второе устройство передаёт его ещё раз.

Если всё прошло удачно, то фрейм передаётся на следующий уровень для обработки.

Межсетевой уровень

Для чего нужен: строить маршруты между устройствами по всему интернету — этот процесс называется маршрутизацией.

Примеры протоколов: IP, ICMP, ARP.

Как работает: IP-протокол вычисляет местонахождение устройств по их IP-адресам, а также строит до них кратчайшие пути и делит данные на пакеты (или, как говорят на юге России, — кульки :)).

Чтобы определить, где находится получатель и как построить путь к нему, IP обращается к системе DNS — она знает IP-адреса всех устройств в интернете.

Когда адрес получен, передаваемый файл разбивается на небольшие части — пакеты. Они содержат фрагменты данных и служебную информацию, например IP-адреса отправителя и получателя.

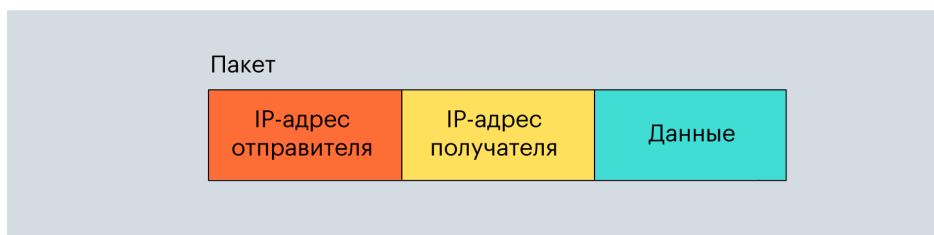


Рисунок 5. Из чего состоит пакет

После этого начинается передача пакетов по маршрутизаторам и коммутаторам. Но процессом отправки занимается уже следующий уровень — транспортный.

Транспортный уровень

Для чего нужен: передавать данные по маршруту, построенному на предыдущем уровне.

Примеры протоколов: TCP, UDP.

Как работает: устанавливает надёжное соединение между устройствами, а затем следит за передачей данных по нему и исправляет ошибки.

Главных протоколов здесь два:

- TCP (Transmission Control Protocol) — гарантирует передачу всех данных без потерь. Полезен при отправке текстовых файлов.
- UDP (User Datagram Protocol) — не гарантирует передачу данных без потерь, но обеспечивает хорошую скорость. Полезен при просмотре видео или прослушивании музыки в интернете.



Рисунок 6. TCP решает всё медленно, но надёжно. UDP — быстро, но не факт, что качественно.

Прикладной уровень

Для чего нужен: настраивать связи между приложениями — например, между браузером и серверным софтом.

Примеры протоколов: HTTP, FTP, SMTP.

Как работает: использует различные протоколы и сервисы, которые помогают приложениям обмениваться данными по интернету.

На прикладном уровне хранятся протоколы для всего, что нужно человеку: отправки имейлов, веб-браузинга, передачи файлов и удалённого доступа. Вот некоторые из них:

HTTP (Hypertext Transfer Protocol) — самый популярный протокол для передачи данных по интернету.

FTP (File Transfer Protocol) — ещё один известный протокол, заточенный под передачу файлов.

SMTP (Simple Mail Transfer Protocol) — протокол для отправки электронных писем.

Этот уровень нужен, чтобы упростить пользователям передачу данных по интернету. Именно с его помощью программисты и обычные пользователи взаимодействуют с моделью TCP/IP.

Слайд 10,11. IP адрес компьютера в сети

Что такое IP-адрес

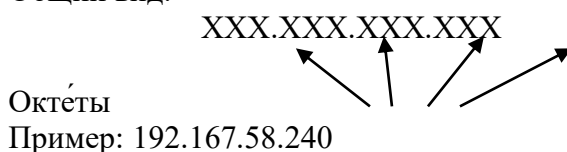
Каждое устройство (ноутбук, компьютер, смартфон) при выходе в интернет получает свой уникальный номер, он присваивается интернет-провайдером и необходим для идентификации информации о хосте (пользователе).

Этот уникальный номер получил название Internet Protocol или сокращенно IP.

IP-адрес — это идентификатор любого устройства, подключенного к интернету. Он всегда уникален и никогда не повторяется. IP — это адрес, по которому можно найти сайт или компьютер. Он состоит из четырех чисел, которые разделены точками, например, 217.69.139.202.

Каждое из четырех чисел, разделенных точками, находится в интервале от 0 до 255. Тогда полный диапазон IP-адресации — адреса от 0.0.0.0 до 255.255.255.255.

Общий вид:



Зачем нужен IP-адрес

Основная задача IP-адреса — распознавать информацию об ее отправителе и получателе в протоколе HTTP (протокол для обмена данными). Откроем для примера сайт NIC.RU. Вы можете узнать место размещения сайта, найдя его IP-адрес по домену, например, через специальный сервис — 31.177.80.4. Таким образом, любой веб-сайт имеет свой уникальный IP-адрес. Вы можете ввести IP в строке браузера и перейти на сайт не используя домен.

Сайту также известен IP, с которого на него заходят, так как ему требуется куда-то отправлять обратную информацию, ответ на запрос, поступивший к нему (а именно — страницы сайта). Например, если мы заходим на сайт международной компании из России, то, определяя страну, из которой пришел запрос, сайт открывается на русском языке (если такие настройки установлены на сайте). Это говорит нам о том, что IP-адрес содержит информацию о географическом местоположении.

Виды IP-адресов

IP-адреса бывают внутренними или внешними.

Внутренний или частный (приватный) IP-адрес используют в локальной сети. Он не виден в интернете, получить доступ к нему можно только в пределах локальной сети. Для внутренних адресов выделен определенный диапазон чисел, которые можно использовать:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Внешний или публичный IP-адрес используется в сети интернет, доступ к оборудованию с внешним IP можно получить из любой точки мира. Каждый из публичных IP-номеров уникален.

Внешние IP-адреса подразделяются на статические и динамические.

Динамические IP-адреса назначаются при каждом новом подключении к интернету и действуют ограниченное количество времени.

Статический IP-адрес закрепляется за устройством, на котором он настроен, и остается неизменным даже при новых подключениях к сети.

Объем привычных адресов IPv4 ограничен и постоянно заканчивается. Для решения этой ситуации были созданы адреса IPv6: если IPv4 имеет 32-битную систему записи, то адреса IPv6 используют 128 бит и представляют собой 8 групп, состоящих из 4 чисел.

Зачем надо знать свой IP-адрес

Каждое устройство, подключаемое к интернету, получает свой индивидуальный номер – IP-адрес. С помощью него можно проследить все действия пользователя в сети.

Зная внешний IP-адрес, вы можете узнать подробную информацию об интернет-провайдере, работать с удаленными системами.

Зная внутренний IP-адрес вы можете видеть все устройства подключенные к вашему роутеру и отслеживать “незаконные” подключения.

Когда вы подключаете дополнительную технику у себя дома, вам может потребоваться IP-адрес для ручной настройки принтера или телевизора с доступом в интернет.

Рассмотрим далее как посмотреть айпи адрес компьютера.

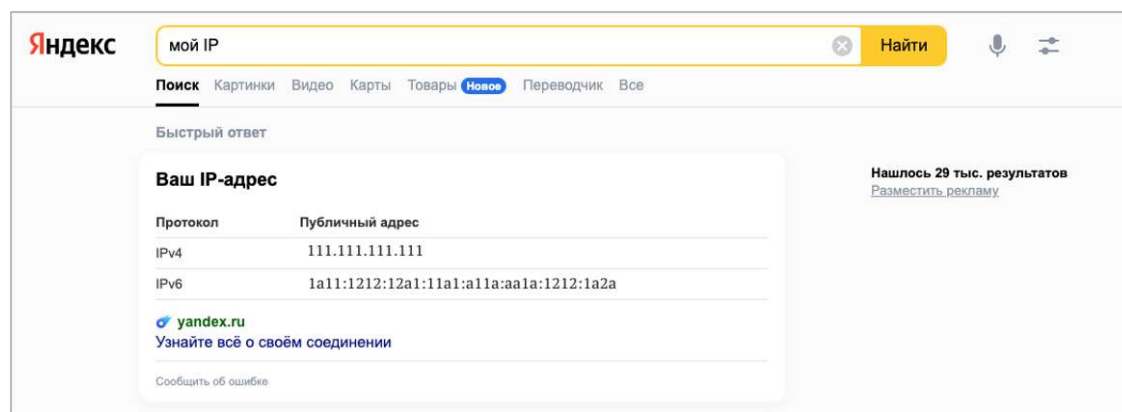
Как узнать внешний IP-адрес

Разберемся как найти ip адрес компьютера. Чтобы узнать внешний IP потребуются сторонние сервисы. Для определения айпи зайдите на один из предложенных сайтов:

На сайте <https://ip.nic.ru/>, где кроме IP вы сможете узнать свою операционную систему, браузер и разрешение экрана.

<https://2ip.ru/> — ваш адрес отобразится на главной странице сайта.

В поисковой строке Яндекса введите Мой IP и нажмите Найти, вам покажутся ваши IPv4 и IPv6 адреса.



Как узнать внутренний IP-адрес

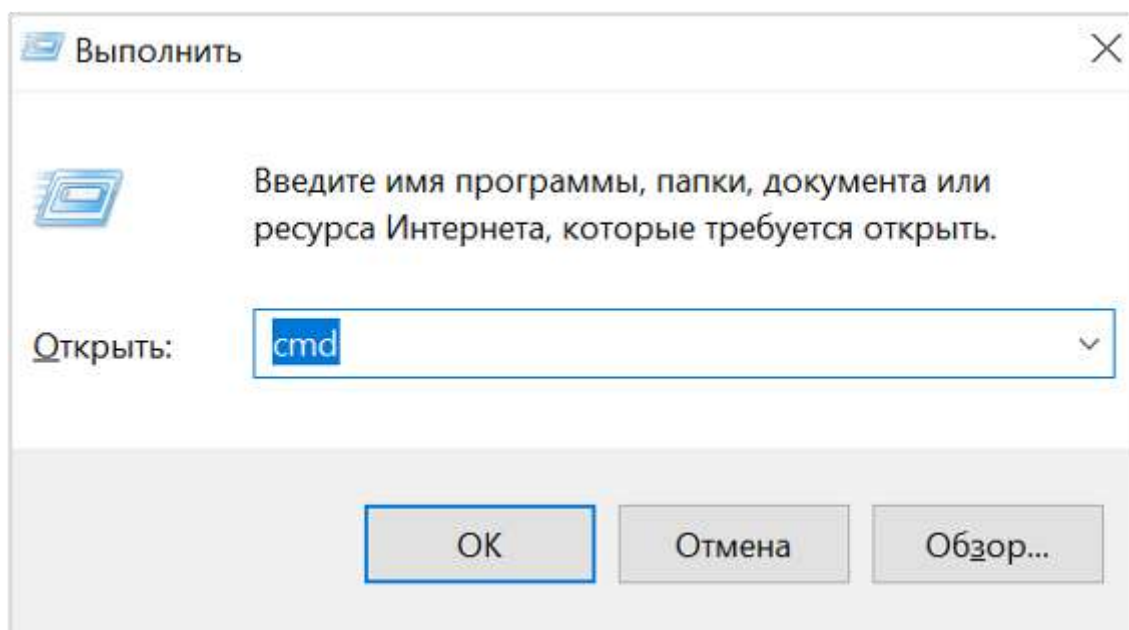
Где посмотреть IP адрес компьютера? Определение IP на устройствах с разными операционными различается.

Если у вас Windows 10, как узнать IP компьютера? Вы можете выбрать один из следующих вариантов:

1. С помощью командной строки
2. Через настройки сети
3. Через диспетчер задач

Как посмотреть IP компьютера с помощью командной строки

Нажмите сочетание Win + R. В открывшемся окне введите cmd и нажмите ОК.



Далее введите команду `ipconfig` и нажмите Enter. В разделе «Адаптер беспроводной локальной сети Беспроводная сеть» вы сможете увидеть свой IP.

```
C:\Windows\system32\cmd.exe
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

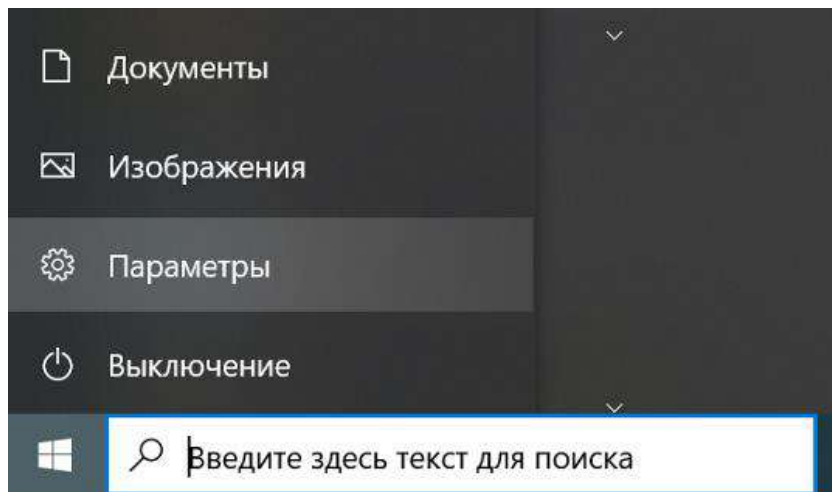
Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

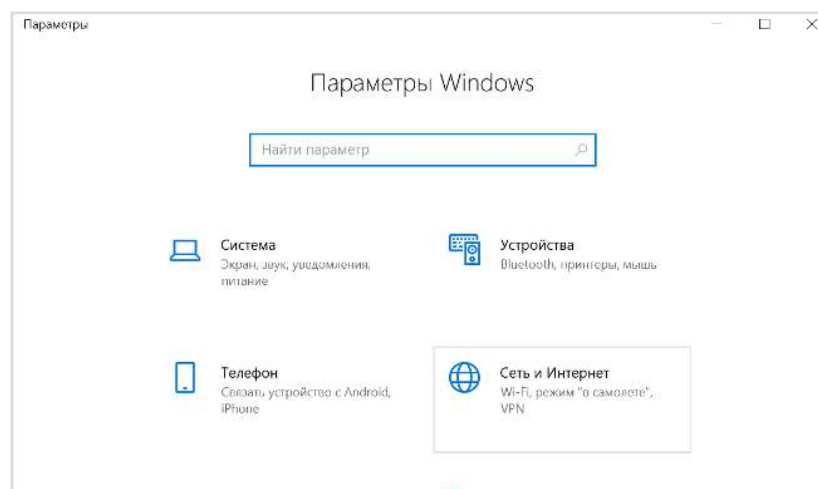
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
IPv6-адрес. . . . . : 2a00
Временный IPv6-адрес. . . . . : 2a00
Локальный IPv6-адрес канала . . . : fe80
IPv4-адрес. . . . . : 192.168.1.1
маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : fe80::1%19
                        192.168.1.1
```

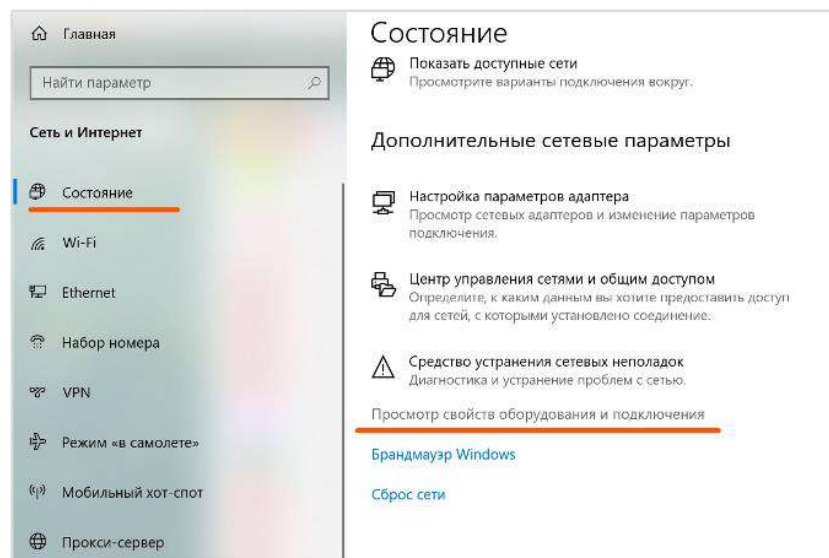
Как узнать айпи адрес своего компьютера через настройки сети
Нажмите на значок Windows и перейдите в раздел Параметры (значок шестеренки).



Откройте Сеть и Интернет и перейдите в раздел Состояние.

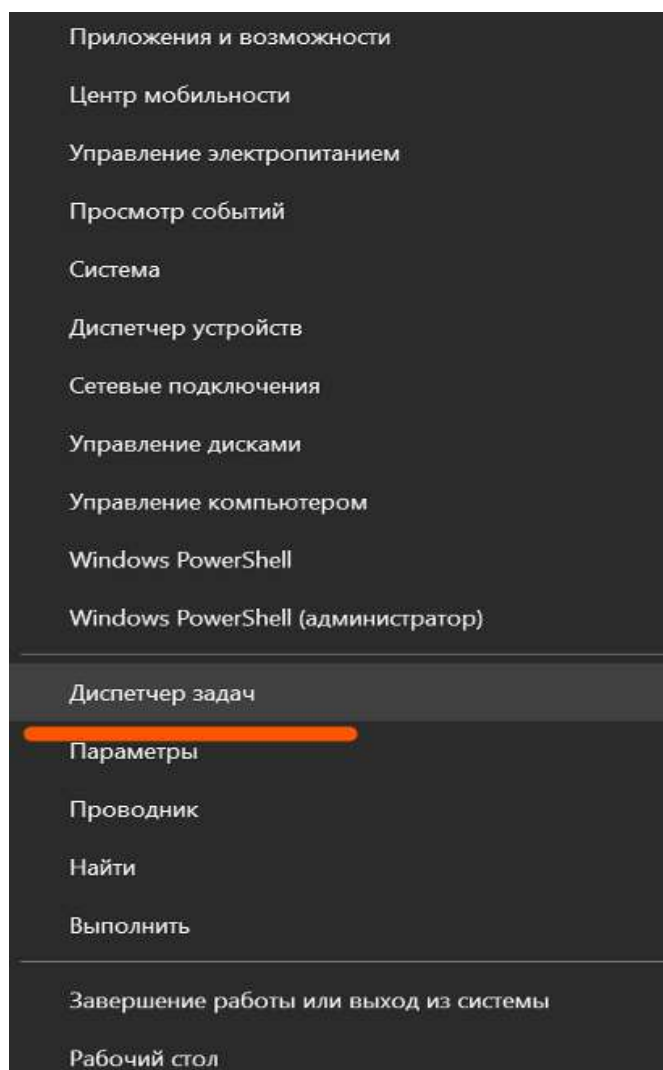


Кликните по ссылке Просмотр свойств оборудования и подключения.

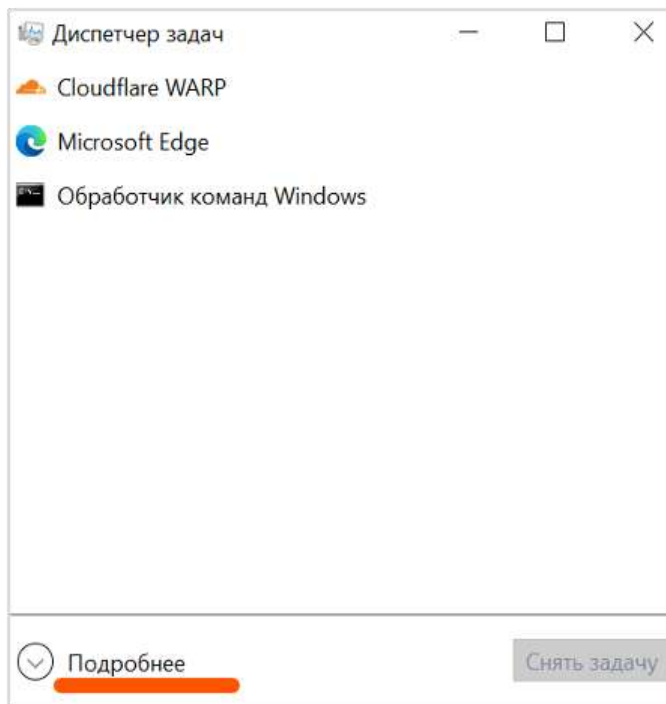




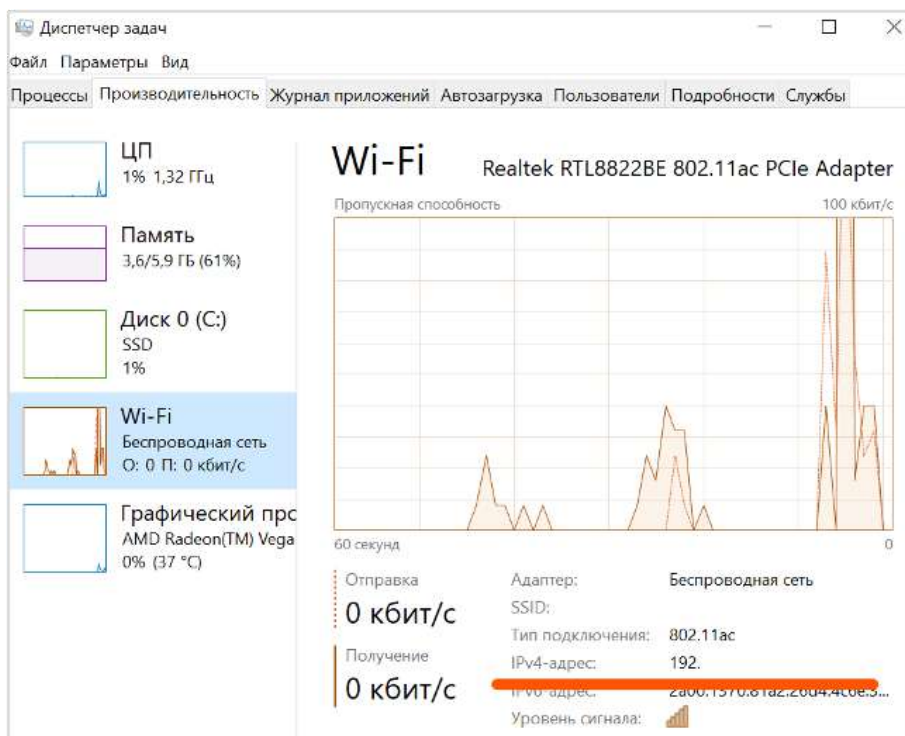
Как найти IP адрес компьютера через диспетчер задач
Щелкните правой кнопкой мыши по кнопке Пуск. В открывшемся меню выберите пункт Диспетчер задач.



Нажмите на ссылку Подробнее и перейдите во вкладку Производительность.



Там перейдите в раздел Ethernet или Wi-Fi, если подключение беспроводное.



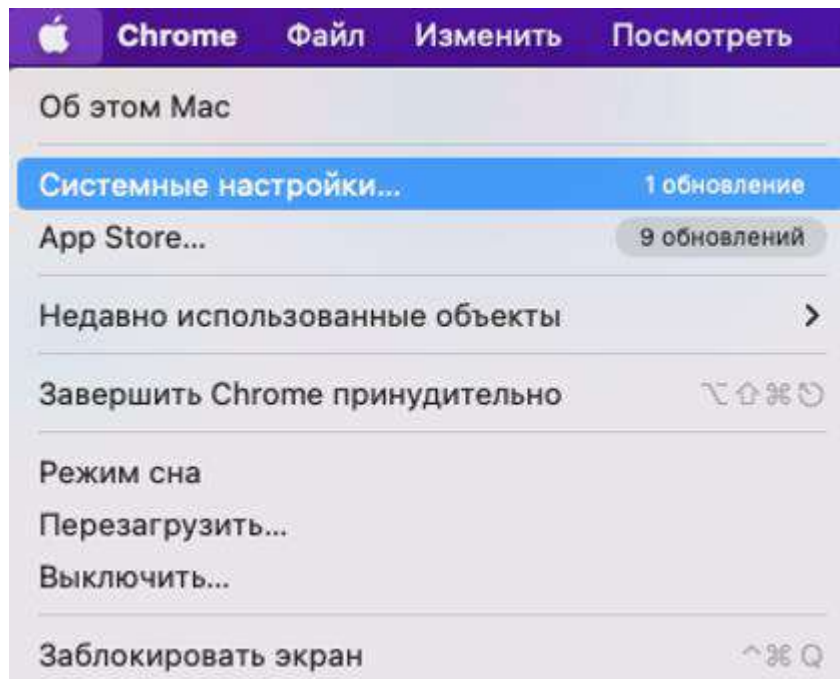
Справа под графиком вы увидите информацию о текущем соединении.

Где найти IP адрес компьютера с macOS

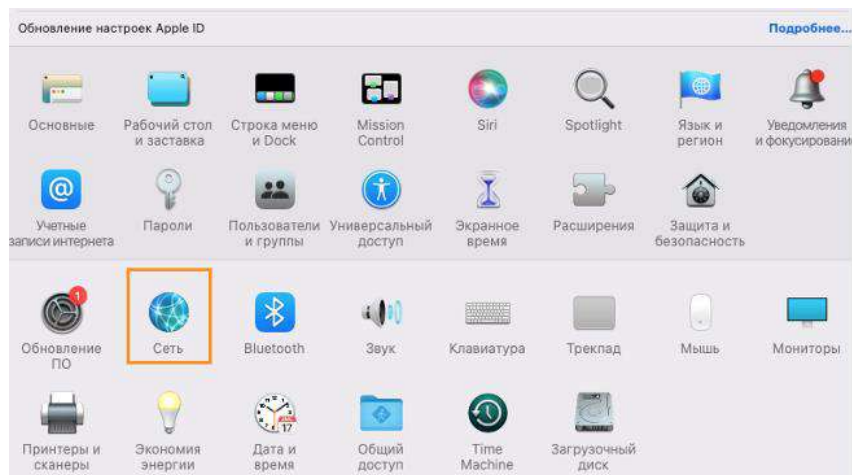
Сделать это можно также тремя простыми способами (инструкция актуальна для ПК, ноутбука, планшета).

Через Системные настройки

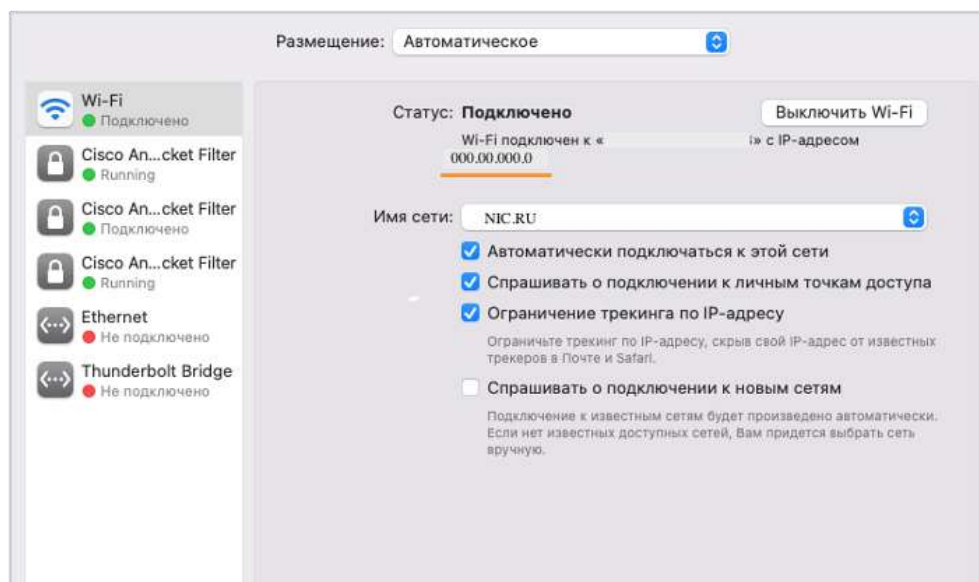
Нажмите на логотип Apple и выберите пункт Системные настройки.



Выберите раздел Сеть.



Вы увидите свой IP-адрес под статусом Подключено.



Через панель меню

Зажимая клавишу Option на клавиатуре, нажмите на знак Wi-Fi меню панели. Ваш IP-адрес появится на табличке с опциями под текущей сетью Wi-Fi.

Через программу Терминал

Откройте раздел Finder и выберите в меню слева пункт Программы

Скролингом или через поиск найдите программу Терминал

Откройте программу и введите команду `ipconfiggetifaddr en0`

Сразу под командой вы увидите свой IP

Если, кроме IP-адреса вы хотите узнать дополнительную информацию, то введите команду `ifconfig |grep inet`. Напротив записи ether вы увидите MAC-адрес, напротив записи inet – IP-адрес.

Можно ли узнать чужой IP-адрес

Без особых усилий вы можете узнать IP любого веб-сайта. Например, это можно сделать с помощью специального сервиса.

Узнать IP-адрес компьютера или другого устройства, выходящего в интернет возможно, но это доступно не каждому. Все данные по айпи адресам есть у интернет-провайдера, но разглашать эту информацию он может только по запросу от правоохранительных органов.

Если вы администратор сайта, то вы можете узнать IP-адреса ваших посетителей: с какого IP они заходили и в какое время. Предположим, с одного и того же адреса вам приходят запросы, которые мешают работе вашего сайта. Вы можете запретить доступ на сайт с конкретного IP-адреса.

IP-адрес обязательная часть коммуникации и передачи данных по интернету, без них работа в сети была бы невозможна.

Хотя многие пользователи не знают свой IP-адрес, такая информация может однажды потребоваться, например, для удаленного доступа или проверки посторонних заходов в ваш аккаунт.

Узнать свой IP достаточно легко и просто. Следуйте приведенным выше инструкциям и поиск IP-адреса не составит для вас большого труда.

Знать IP компьютера, не только своего, но и чужого не запрещено. Нельзя применять технические способы сокрытия своего адреса или поиска IP другого пользователя с целью незаконных действий.

Информация в раздаточном материале. Компьютерные сети могут объединять различное количество абонентов, есть сети большие и маленькие. Для того, чтобы наиболее рационально распределять адреса, их разделили на три класса: А, В, С.

Первые биты адреса указывают на тип класса, последующие на адрес сети, и последняя группа – адрес компьютера в сети.

Подробнее можно посмотреть в таблице:

Класс А	0	Адрес сети (7 битов)		Адрес компьютера (24 бита)
Класс В	1	0	Адрес сети (14 битов)	Адрес компьютера (16 битов)
Класс С	1	1	0	Адрес сети (21 бит)
				Адрес компьютера (8 битов)

Получается, что сети класса А большие, каждая может содержать $2^{24} = 16777216$ компьютеров, но таких сетей мало ($2^7 = 128$), всего 128 сетей.

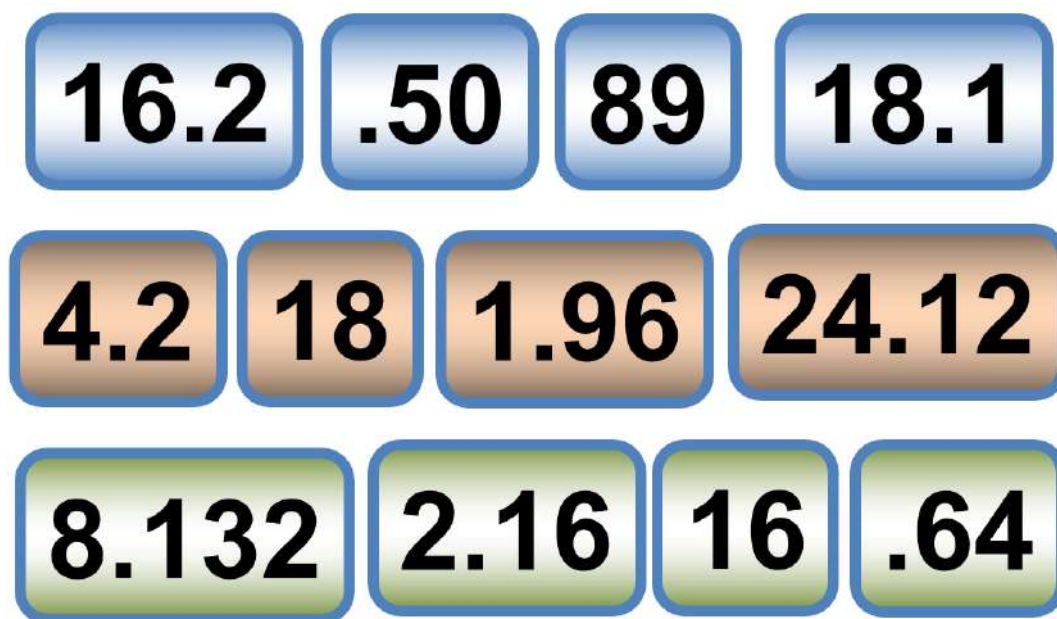
А вот сети класса С – маленькие, могут содержать до 256 компьютеров, зато их может быть очень много.

Чтобы определить класс сети, достаточно посмотреть на первое число в ip-адресе:

класс А – число от 0 до 127;

класс В – число от 128 до 191;

класс С – число от 192 до 223.



Слайд 12.

Пример IP – адреса

IP-адреса могут быть *статическими* и *динамическими*. Для сервера, на котором хранится информация, необходим постоянный IP-адрес, иначе данные не будут найдены. Для пользователя, входящего в Интернет на несколько часов, IP-адрес может быть выделен динамически из некоторого количества имеющихся у провайдера свободных номеров. По желанию пользователь может иметь и постоянный IP-адрес

Слайд 13,14,15

Решение задач

Слайд 13. 16.218.189.50

Слайд 14. 184.224.121.96

Слайд 15. 162.168.132.64

Слайд 16.

Пауза для отдыха

Выполнение упражнений

5. **Самостоятельная работа обучающихся с информацией, представленной в печатном виде.**

Слайд 17

Доменная система имен.

Прочитайте информацию по теме «Доменная система имен». Выпишите в тетрадь определения, встречающиеся в тексте.

Домен – это группа компьютеров, объединенных по некоторому признаку.

Числовые адреса – единственно возможный метод идентификации для компьютеров, но для пользователей Интернет они неудобны, поскольку не несут смысловой нагрузки, а значит, практически не запоминаются. Поэтому в Интернете предусмотрена возможность использования их аналогов в текстовом представлении. Это так называемые *доменные адреса DNS* (DomainNameSystem).

Доменная система имен ставит в соответствие числовому IP-адресу каждого компьютера уникальное доменное имя.

Доменная система имен имеет иерархическую структуру:



В отличие от IP-адресов, мало говорящих пользователю, кому принадлежит и где находится ресурс Интернет, доменные имена несут много полезной информации.

Расшифровку доменного имени легко провести, читая его составляющие справа налево.

В любом имени справа записывается *домен первого уровня*, состоящий из двух, трех или четырех букв. Он означает страну или принадлежность к определенной деятельности. Количество имен первого уровня ограничено.

Домены 1-ого уровня (доменные зоны)

Вид организации	Страна
.comкоммерческие организации	.ruРоссия
.eduобразование	.uaУкраина
.gov правительство и его органы	.byБелоруссия
.mil военные организации	.ukВеликобритания
.org, разные неком. организации	.itИталия
.info информационные сайты	.jpЯпония
.biz бизнес	.cnКитай
.net общественные ресурсы	.usСША

Пространство доменных имен имеет иерархическую структуру
Корневой домен располагается на самом верху иерархии и обозначается точкой.



Домены верхнего уровня создаются по определенному признаку. В них объединяются компьютеры сети по географическому признаку или роду деятельности. Например:

ru, uk и т.д. - определяют географическое положение (ru - Россия, uk – Украина)
com - коммерческие организации (например, microsoft.com);
edu - образовательные (например, mit.edu);
gov - правительственные организации (например, congress.gov);
org - некоммерческие организации (например, rfc-editor.org);
net - организации, поддерживающие части сети Internet (например, nsf.net).

Домены второго уровня обычно относятся к названиям компаний и регистрируются владельцами доменов верхнего уровня.

Домены третьего уровня обычно относятся к подразделениям внутри компаний. При формировании имени домена к нему добавляется имя родительского домена. Например, домен второго уровня microsoft.com, домен третьего уровня eng.microsoft.com.

Домены ниже третьего уровня, как правило, встречаются редко.

Сначала InterNIC – организация, ответственная за систему имен – ввела в обращение семь доменных имен первого уровня. Т.к. система доменных имен впервые появилась в США, то эти семь доменов по умолчанию означают, что хост расположен на территории США.

Слева от имени домена первого уровня записывается одно или несколько имен доменов второго, иногда третьего и более низких уровней.

Имя домена второго уровня выбирается компанией и несет информацию о ее названии или услугах, имя домена третьего уровня может означать подразделение этой компании.

И, наконец, слева в доменном имени стоит имя компьютера, на котором хранится информация.

Например, www.microsoft.com означает, что компьютер (сервер) с именем www находится в домене Microsoft, который входит в домен первого уровня .com.

Домены верхнего уровня бывают двух типов:

1. *географические* (двухбуквенные) – каждой стране соответствует двухбуквенный код;
2. *административные* (трехбуквенные) – позволяет определить профиль организации, владельца домена.

Вот некоторые имена доменов верхнего уровня

Административные	Тип организации	Географические	Страна
com	коммерческая	ca	Канада
edu	образовательная	de	Германия
gov	правительственная	jp	Япония
int	международная	ru	Россия
mil	военная	su	Бывший СССР
net	компьютерная сеть	uk	Англия/Ирландия
org	некоммерческая	us	США

В имени компьютера может быть любое число доменов, но, как правило, 2–4.

Компьютеры используют IP-адреса, для людей удобней и понятней доменные имена. Следовательно, должен существовать механизм преобразования вводимых пользователем доменных имен в IP-адреса. Этим занимается *служба доменных имен Интернет – DNS (DomainNameService)*.

Работа службы имен состоит в том чтобы, получив от пользователя доменное имя, отыскать соответствующую ему запись в таблице DNS – распределенной базе данных, хранящейся на тысячах компьютерах в сети. Найденный IP-адрес возвращается на компьютер пользователя, пославший запрос. И только после этого по IP-адресу запрашивается информация из Интернета. Система серверов DNS представляет собой тысячи компьютеров с определенной иерархией.

Службы Internet

Изначально в Internet было создано три основные службы: удаленный доступ, пересылка файлов и электронная почта (обмен сообщениями). Потом появились другие службы и продолжают появляться все новые. Практически все службы используют технологию «клиент-сервер», при которой для функционирования каждой службы должен существовать сервер (сервера), а клиенты должны пользоваться специальным клиентским ПО для доступа к серверу.

Удаленный доступ (TELNET)

Telnet позволяет подключиться со своего компьютера к удаленному компьютеру (на котором работает telnet сервер) и стать его терминалом (устройством ввода-вывода). При этом вся обработка информации происходит на удаленном компьютере (его процессором и в его оперативной памяти), ввод команд осуществляется с вашей клавиатуры, вывод результатов – на ваш дисплей. При подключении к удаленному компьютеру необходимо зарегистрироваться в его ОС – вести правильные имя и пароль.

Удаленный доступ позволяет работать в своей компьютерной системе с помощью любого компьютера, подключенного к Internet. Таким же образом реализовано использование суперкомпьютеров в сети. В состав Windows входит программа telnet, являющаяся клиентским ПО удаленного доступа.

Перемещение файлов (FTP)

Найдя нужную информацию в Internet или проведя расчеты на удаленном компьютере необходимо перенести информацию на свой компьютер. А перед началом расчетов надо по крайней мере передать на удаленный компьютер исходные данные. Для этого предназначен File Transfer Protocol (протокол передачи файлов) – FTP. В качестве клиентской программы можно использовать поставляемую с Windows программу ftp (с интерфейсом – «командная строка») или одну из бесплатных или условно-бесплатных программ (например, CuteFTP). Протокол FTP также доступен из Internet браузера. Во время сеанса связи происходит подключение к FTP серверу, для чего надо знать имя и пароль. Многие сервера допускают «анонимное» подключение, когда в качестве имени пользователь указывает «anonymous», а в качестве пароля – свой адрес электронной почты (иногда его проверяют на подлинность). Администратор сервера может устанавливать различные полномочия для разных пользователей, в том числе минимальные – для анонимного доступа.

Некоторые клиентские программы требуют явного указания режима передачи: двоичный (Binary) или ASCII (другие выбирают режим самостоятельно). При двоичном режиме передачи файла сохраняется последовательность битов исходного файла. В режиме ASCII пересылаемые данные рассматриваются как символы, которые должны сохранять свой смысл в разных операционных системах (UNIX, DOS, Macintosh, SVM, etc.). Поэтому двоичный режим следует использовать для пересылки исполнимых файлов (программ), графических файлов, архивов, а режим ASCII – для пересылки текстов, сообщений электронной почты и др.

Подключившись к серверу с помощью клиентской программы пользователь получает возможность (в рамках отведенных ему полномочий) загружать файлы с сервера на свой компьютер (Download), отправлять файлы со своего компьютера на сервер (Upload), а также переименовывать и удалять файлы, перемещаться по дереву каталогов и создавать свои каталоги на сервере (часто запрещено). Иногда можно даже запускать файлы на выполнение на сервере (почти telnet).

Электронная почта (e-mail)

Электронная почта предназначена для обмена текстовыми сообщениями между пользователями подключенных к Internet компьютеров.

Вместо конверта для сообщения используется заголовок, содержащий по крайней мере три обязательных поля: To (Кому), From (От кого) и Subject (Тема). Поля To и From содержат электронный адрес получателя / отправителя. Из-за взаимодействия в Internet разных сетей адреса могут записываться по-разному. Угадать адрес невозможно, поэтому следует хранить полезные адреса в «адресной книге».

Большинство адресов имеют следующий формат:

имя_пользователя @ имя_почтового_сервера

Например: info@elmech.mpei.ac

Задача Internet службы «электронная почта» – доставить сообщение на почтовый сервер адресата. Пользователь должен самостоятельно «проверять почтовый ящик» и забирать пришедшую почту с сервера с помощью клиентской почтовой программы (она же «отправляет» исходящие почтовые сообщения). В состав Windows входит клиентская программа Exchange, а в пакет Office – программа Outlook. Кроме того, почтовый клиент поставляется вместе с пакетом Netscape Communicator. Большой популярностью также пользуется программа The Bat:

Пересылка файлов

К сообщениям электронной почты можно «прикреплять» файлы и пересылать их без использования протокола FTP. Но! Некоторые провайдеры ограничивают размер почтовых сообщений или взимают дополнительную плату за каждый килобайт информации. Кроме того, электронная почта предназначена для передачи текстовых сообщений, поэтому при пересылке двоичных файлов происходит их кодирование / декодирование. При этом важно, чтобы отправляющая и принимающая стороны использовали одинаковые стандарты кодировки (uuencode/uudecode, binhex). Сейчас большинство систем поддерживают стандарт MIME (Multi-purpose Internet Mail Extensions), что значительно облегчает «взаимопонимание» при пересылке файлов. Однако, надежнее все же пересылать файлы, запакованные в архивы (самый популярный – ZIP). Внутри архива никто файл не перекодирует по дороге.

Возврат почты

При невозможности доставить почту отправителю приходит служебное сообщение с отказом. Можно выделить три основные причины отказа:

Host unknown – доменное имя компьютера (почтового сервера) невозможно преобразовать в адрес – проверьте правильность написания имени компьютера;

User unknown – пользователь (почтового сервера) неизвестен – проверьте правильность написания имени пользователя;

Service unavailable или Cannotsendmessagefor ... days – не работает почтовый сервер адресата (нет связи или отключено ПО почтового сервера).

Телеконференции (News)

Коллективные дискуссии можно проводить с помощью списков рассылки и электронной почты, но при большом числе подписчиков это становится сложно. Кроме того, приходящие сообщения смешиваются со служебными, что мешает работе. Для свободных дискуссий создана служба телеконференций («новости», «эхо»). Там все сообщения сортируются по темам и каждый может выбирать только те темы, которые ему интересны. Кроме того, все сообщения хранятся на сервере (news-server) и каждый пользователь может читать (загружать на свой компьютер) только те, которые ему интересны (выбирая по полю subject в заголовке). При этом сохраняется возможность отвечать на выбранные сообщения или отправлять свои в режиме общения «каждый – со всеми».

Для работы с телеконференциями необходима клиентская программа (подобные программы входят в состав пакетов Netscape Navigator или Internet Explorer, а также выпускаются самостоятельно). При первом вызове программы пользователь должен указать имя сервера, подключившись к которому он может вывести полный список рубрик (тем),

поддерживаемых данным сервером (определяется администратором сервера). Из этого списка можно выбрать интересные (подписаться) и в дальнейшем заголовки сообщений из этих рубрик программа будет запрашивать с сервера автоматически при каждом подключении. Рубрики имеют иерархическую структуру: существуют рубрики верхнего уровня, в каждой из которых могут быть свои подгруппы, конкретизирующие тему дискуссии, и т.д. Разные уровни в названии рубрик отделены точкой, верхний уровень записан слева. Например: rec.music.folk – recreation – music – folk music.

Поискфайлов (Archie)

Известно, что в Internet на общедоступных FTP серверах расположено огромное количество файлов с документами, графикой и полезными программами. Но для того, чтобы скачать себе нужный файл, необходимо сначала узнать его «адрес» – имя сервера, путь и имя файла. Для поиска файлов на FTP серверах всего Internet создана служба Archie. Эта служба впервые появилась в университете McGill, но потом число archie серверов стало расти.

Каждый archie сервер регулярно (примерно раз в месяц) запускает программу сбора информации, которая подключается ко всем общедоступным FTP серверам, собирает всю информацию о находящихся в данный момент на сервере файлах и помещает ее в свою базу данных. При поступлении от клиента запроса на поиск определенного файла archie сервер производит поиск в своей базе данных (что выполняется достаточно быстро) и выдает список отвечающих запросу файлов с указанием их точных «адресов». При этом надо помнить, что такая информация постоянно устаревает, поэтому следует использовать данные разных archie серверов и проверять аналогичные файлы, расположенные на разных FTP серверах.

Для обращения к серверу Archie необходимо использовать специальную клиентскую программу или воспользоваться WWW интерфейсом, что гораздо удобнее (см. ниже). В запросе следует указать точное имя файла или его часть. Иногда можно найти файл по ключевым словам из его описания (если, конечно, FTP сервер содержит описания файлов). В последнем случае можно воспользоваться дополнительной командой whatis для получения имеющегося комментария к файлу.

Поиск ресурсов(Gopher)

Под ресурсами понимают сразу все, что может находиться в Сети: различные серверы, адреса пользователей, программы, графические и музыкальные файлы, новости и пр.

Система Gopher позволяет просматривать список всех доступных ресурсов сервера и сама организует правильный доступ к разным ресурсам с помощью системы меню. Как правило, она содержит ссылки на другие сервера с подобной системой. Именно такая система активизируется при подключении по telnet к Библиотеке Конгресса США. В последние годы эта система не развивается, так как то же самое позволяет делать самая популярная служба – WWW.

World Wide Web

WWW создана в 1989 г. В Европейской лаборатории физики элементарных частиц (CERN) Женева, Швейцария. Ее автор TimBerners-Lee (из Оксфордского университета) создал информационную систему для упрощения сотрудничества ученых и обмена документами.

WWW использует технологию гипертекста для объединения во взаимосвязанную систему большого количества документов, между которыми можно перемещаться в произвольном порядке для поиска нужной информации. Документы хранятся на WWW серверах. Для просмотра документов и перемещения между ними используется клиентская программа – браузер (browser).

Изначально браузер был только текстовый (Lynx) и поддерживал любые типы мониторов и мог работать на любых компьютерах. В 1993 г. Mark Andreessen (студент Университета штата Иллинойс, подрабатывавший в Национальном центре суперкомпьютерных технологий – NCSA) создал первый графический браузер – NCSA Mosaic, который был способен отображать на экране одновременно текст и графику. Кроме графики браузер отличался

интуитивно понятным интерфейсом – гипертекстовый переход осуществлялся по щелчку мыши.

Появление службы WWW и графического броузера сделало Internet интересным и доступным для миллионов людей, далеких от науки. Internet стали использовать для развлечений, что способствовало инвестициям и дальнейшему развитию Internet технологий. Основу службы WWW составляет технология гипертекста. В обычной бумажной книге реализован линейный подход к публикации: страницы идут одна за другой, оглавление позволяет ориентироваться в структуре книги. В гипертекстовом документе существуют связи между отдельными частями документа или между разными документами, позволяющие быстро переходить от одного материала к другому. Причем, наличие логической связи между документами совсем не обязательно – на все воля автора. Именно принцип случайности в установлении связей обеспечивает объединение даже разнородных документов в единую систему WWW. Упрощенный вариант гипертекстового документа реализован в справочных системах многих программных продуктов, содержащих «перекрестные ссылки».

В WWW возможны ссылки на участки того же документа, на другие документы, расположенные на том же сервере, или на документы других серверов. Кроме того, ссылки могут указывать на текстовые, графические, архивные или мультимедийные файлы или представлять собой запрос к archie серверу.

В WWW применена обычная технология «клиент-сервер».

Клиент (броузер) принимает запрос пользователя («перейти по этой ссылке»), обращается к соответствующему серверу и запрашивает у него требуемый документ. Получив документ, броузер интерпретирует его и показывает пользователю. Обычно броузер показывает текст и графику (файлы графических форматов GIF и JPEG). Но различные вспомогательные программы позволяют воспроизводить прямо в окне броузера звуковые файлы или видео. К сожалению, разные броузеры могут по разному интерпретировать один и то же документ.

Web сервер предназначен для хранения документов и передачи их броузеру при получении соответствующего запроса. Кроме того, сервер может по запросу броузера запускать на выполнение различные программы: обращение к базе данных с запросом на поиск информации, занесение в базу данных информации пользователя, просто подсчет числа обращений к определенному документу).

Документы в WWW представляют собой простые текстовые файлы, содержащие помимо собственно текста специальные метки, которые описывают вид и структуру документа. Метки должны соответствовать языку гипертекстовой разметки HTML (HyperTextMarkup Language). Такие документы называются HTML документами.

Броузер, получив текстовый файл с HTML документом, начинает интерпретировать его, представляя информацию в своем окне в соответствии с обнаруженными метками. Метки позволяют выделять в тексте заголовки разного уровня, организовывать списки, таблицы и, главное, создавать ссылки на другие документы.

Для организации ссылки на любой документ в Сети используется глобальная адресация документов. Каждый документ, размещенный на Web сервере имеет уникальный адрес – URL (Universal Resource Locator). URL в общем случае состоит из четырех частей: имени протокола, который должен использоваться для обращения к данному документу, имени (или IP адреса) Web сервера, на котором расположен документ, пути в структуре каталогов сервера и собственно имени файла. Например:

elmech.mpei.ac/em/frame_win.html

Здесь описывает протокол (HyperText Transfer Protocol);

elmech.mpei.ac – представляет собой имя Web сервера;

/em – путь;

frame_win.html – имя файла.

Навигация в WWW

WWW представляет собой совокупность взаимосвязанных документов. HTML документы еще называют «страницами». Как правило авторы не ограничиваются одной страницей, а создают «сайт» – набор из нескольких страниц со взаимными ссылками, логически объединенных одной темой. Каждый Web сервер может содержать любое число сайтов, но чаще он посвящен только одной «теме». Ниже рассмотрены разновидности сайтов, наиболее популярные в Internet в последнее время.

Личная домашняя страница – самый простой и распространенный тип страниц, разновидность «визитной карточки». Содержит любую информацию об авторе: личные сведения, увлечения, коллекции ссылок. Примеры можно посмотреть здесь: www.mpei.ac/homer

Тематическая страница – создается энтузиастом и содержит сведения о его увлечении, любимом музыканте, актере и т.д. Часто «официальными» страницами называют те, содержание которых одобрено лицом, которому она посвящена. Иногда такие страницы создаются группами энтузиастов и описывают общие увлечения, например, www.moto или www.fishing

Электронные средства информации-либо электронная (Internet) версия традиционного издания, либо чисто Internet издание (существующее только в Сети). Могут обновляться ежедневно (или даже чаще), раз в месяц или реже. Они используют такие преимущества сетевых изданий, как оперативность подачи информации, отсутствие цензуры, относительная дешевизна издания. Многие живут только за счет размещения рекламы. Пример: www.gazeta

Электронное представительство компании – иногда просто лишний способ заявить о своем существовании, но чаще это информация о профиле компании, выпускаемых продуктах (услугах), наличии товаров на складе (в магазине) и их ценах, иногда есть возможность сделать заказ. Пример: www.mvideo

Internet магазин – сайт, содержащий не только информацию о товарах и их ценах, но позволяющий также произвести покупку товара с оплатой по кредитной карточке или наличными и последующей доставкой. Пример: www.dostavka

Портал – сайт, претендующий на роль «ворот» («портала») в мир Internet. Он содержит свежие новости, ссылки на электронные средства информации, представительства компаний и организаций, сам является каталогом ресурсов и т.д. и т.п. Пример: www.km

Протоколы сети Internet

Основное, что отличает Internet от других сетей - это ее протоколы - TCP/IP. Вообще, термин TCP/IP обычно означает все, что связано с протоколами взаимодействия между компьютерами в Internet. Он охватывает целое семейство протоколов, прикладные программы, и даже саму сеть. TCP/IP - это технология межсетевого взаимодействия, технология internet. Свое название протокол TCP/IP получил от двух коммуникационных протоколов (или протоколов связи). Это Transmission Control Protocol (TCP) и Internet Protocol (IP). Несмотря на то, что в сети Internet используется большое число других протоколов, сеть Internet часто называют TCP/IP-сетью, так как эти два протокола, безусловно, являются важнейшими. Как и во всякой другой сети в Internet существует 7 уровней взаимодействия между компьютерами:

физический,

логический

сетевой

транспортный

уровень сеансов связи

представительский

прикладной уровень

Соответственно каждому уровню взаимодействия соответствует набор протоколов (т.е. правил взаимодействия).

Протоколы физического уровня определяют вид и характеристики линий связи между компьютерами. В Internet используются практически все известные в настоящее время способы связи от простого провода (витая пара) до волоконно-оптических линий связи (ВОЛС).

Для каждого типа линий связи разработан соответствующий протокол логического уровня, занимающийся управлением передачей информации по каналу. К протоколам логического уровня для телефонных линий относятся протоколы SLIP (Serial Line Interface Protocol) и PPP (Point to Point Protocol). Для связи по кабелю локальной сети - это пакетные драйверы плат ЛВС.

Протоколы сетевого уровня отвечают за передачу данных между устройствами в разных сетях, то есть занимаются маршрутизацией пакетов в сети. К протоколам сетевого уровня принадлежат IP (Internet Protocol) и ARP (Address Resolution Protocol).

Протоколы транспортного уровня управляют передачей данных из одной программы в другую. К протоколам транспортного уровня принадлежат TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). Протоколы уровня сеансов связи отвечают за установку, поддержание и уничтожение соответствующих каналов. В Internet этим занимаются уже упомянутые TCP и UDP протоколы, а также протокол UUCP (Unix to Unix Copy Protocol). Протоколы представительского уровня занимаются обслуживанием прикладных программ. К программам представительского уровня принадлежат программы, запускаемые, к примеру, на Unix-сервере, для предоставления различных услуг абонентам. К таким программам относятся: telnet-сервер, FTP-сервер, Gopher-сервер, NFS-сервер, NNTP (Net News Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP2 и POP3 (Post Office Protocol) и т.д. К протоколам прикладного уровня относятся сетевые услуги и программы их предоставления.

Защита информации в интернете

Сегодня Интернет – это основа работы многих компаний, способ мгновенно обмениваться информацией, вести переговоры, совершать покупки. Практически каждый человек ежедневно использует сеть в личных целях или для работы, оставляет в ней свой след и пересылает информацию, которую хотел бы оставить конфиденциальной.

Защита информации в Интернете – это одна из основных забот большинства предприятий. Ведь соблюсти баланс между применением эффективных методов и удобством сотрудником при работе не всегда просто. Однако система необходима, чтобы избежать финансовых и репутационных потерь.

Риски при использовании незащищенного интернета. Заранее точно предсказать, как именно пострадает конкретный пользователь или целая организация, не обратившая должное внимание **на систему защиты информации** в Интернете, практически невозможно. Существуют сотни различных вариантов совершения преступлений, в основе которых чаще всего лежит комбинация из незаконных действий.

Наиболее распространенными рисками считаются:

- Получение доступа к закрытой информации без каких-либо санкций.
- Кража важных данных компании или конкретного человека.
- Подмена или внесение изменений в информацию при ее передаче или в период содержания в хранилище.
- Удаление важных данных в качестве злого умысла.
- Разглашение незаконно полученных данных.
- Намеренное шифрование информации с целью последующего шантажа и вымогательства.

Организация системы должна в первую очередь учитывать **три основные проблемы защиты информации в Интернете:**

- Человеческий фактор. В большинстве случаев виновниками утечки становятся сами люди.
- Методики передачи. Необходимо выбирать наиболее защищенные.

- Способы хранения баз данных.

Также при решении этого вопроса в каждой организации должны учитываться все соответствующие положения ФЗ-149 «Об информации, информационных технологиях и о защите информации».

Кому грозит опасность?

От незаконных действий злонамеренных элементов в сети может пострадать как простой человек, так и крупная компания. Каждый, кто хоть раз в жизни вел социальные сети или заказывал что-то через интернет, регистрировался на сайте и предоставлял информацию о себе, может стать жертвой мошенников. Частному лицу есть чего опасаться: Создание фиктивной личности с вашими данными для ведения незаконной деятельности. Нанесение ущерба личной репутации при опубликовании конфиденциальных материалов. Разрушение репутации человека действиями якобы от его имени: продажа недвижимости, товаров, оформление кредитов, неоднозначные высказывания. Сегодня действует закон о защите персональных данных в сети, и каждый портал, на который мы вносим свои данные, должен его соблюдать. Однако это не снимает ответственности лично с нас. Безопасность личной информации в интернете, прежде всего, забота конкретного пользователя. Страдают от мошенников и компании. При этом им может быть нанесен конкретный урон, который в иных случаях оборачивается полным крахом для всей организации. Наиболее распространенные случаи противозаконного использования доступа: Промышленный шпионаж. Полученную информацию продают конкурентам, тем самым значительно снижая прибыли фирмы. Раскрытие стратегических данных. В том числе ближайшие планы по развитию компании в том или ином направлении. Изменение качества изготавливаемого товара. Для этого необходимо лишь удаленно заменить настройки оборудования, описание процесса производства или требования к первоначальному сырью. Срыв договорных обязательств. Часто это происходит из-за изменений в сроках логистики, в качестве поставляемого продукта или сроках выполнения заказанных работ. Прямой шантаж или вымогательство. Кража данных или их шифрование с целью получения выгоды подобным путем – распространенное явление на территории нашей страны. Приведенные ситуации – лишь малая, хотя и самая популярная, доля того, что могут сделать злоумышленники, если получат доступ к хранилищам данных или смогут их перехватывать при отправке. Именно поэтому разнообразные современные способы защиты информации в Интернете вызывают особый интерес среди бизнесменов. Особенно актуальным этот вопрос стал в связи с достаточно распространенной практикой перехода многих сотрудников на удаленную работу. Основные методы защиты

Конкретный список мер, которые используются для защиты от злоумышленников в сети, выбирает каждая компания для себя самостоятельно. При этом в обязательном порядке должны учитываться требования закона. Система защиты информации в Интернете создается с помощью применения целого комплекса различных методов, которые можно разделить на несколько категорий.

Программные

Это наиболее широкая область, позволяющая подобрать индивидуально наиболее подходящие пакеты в конкретном случае. Выбираемые способы напрямую зависят от используемых в работе программ, онлайн платформ, операционной системы и принятой механики доступа. Общепринятые защитные меры, которые способны обеспечить различные программы: Управление доступом. Включают как программные, так и непосредственно аппаратные методы. Обеспечивают возможность работы только для конкретных лиц. Разнообразные комплексы шифрования. Электронные ключи – распространенную систему подтверждения подлинности самих данных и возможности доступа, целый ряд вспомогательных программ для работы с ними. Система, отслеживающая попытки несанкционированного проникновения к базам или прямые атаки на них. Подобранные с умом программные методы защиты позволяют практически полностью исключить возможность взлома информационных хранилищ, получение незаконного доступа к данным.

Кроме того, они включают и стандартные методы шифрования информации при непосредственной передаче, особенно происходящей в пределах общей платформы.

Аппаратные

Являются важнейшей частью создания безопасной среды, позволяющей спокойно работать при подключении к сети Интернет и не только. Именно им уделяется наибольшее внимание при формировании цифровой среды организации. Их задачи обширны: Непосредственно обрабатывать запросы зарегистрированных пользователей. Поддерживать высокую скорость доступа к данным на серверах. Сохранить работоспособность и целостность оборудования даже в случае отключения электроэнергии. Для этого используются дополнительные генераторы или источники бесперебойного питания. Обеспечить сохранение всех данных даже при выходе из строя части техники или конкретных средств хранения. Сокращение и полное устранение ущерба в случае воздействия внешних факторов непреодолимой силы. Особенно актуально в случае возникновения пожаров или попытках физического уничтожения техники. Создание резервных копий и быстрый доступ к ним в случае необходимости. Обеспечение постоянных средств связи для каждого сотрудника. В той или иной мере в обязательном порядке используется принцип дублирования основных систем, что позволяет быстро восстановить работу в случае возникновения форс мажорных обстоятельств. Дополнительную защиту информации в Интернете обеспечивают межсетевые экраны, программный доступ к сети, современные системы идентификации сотрудников.

Смешанные

Эти методы актуальны при необходимости обеспечить разноуровневый доступ для различных сотрудников, а также отслеживание их деятельности и дополнительный контроль. К наиболее распространенным и используемым практически в любой компании относятся: Антивирусы. Стандартное шифрование информации при передаче. Различный уровень доступа к данным для сотрудников одной группы. Система идентификации работников, в том числе реализующаяся аппаратно. Именно к этим способам защиты информации в Интернете относятся составление наиболее безопасных схем взаимодействия сотрудников друг с другом и мониторинга процесса работы. Организационные Самым распространенным способом получить доступ к необходимой информации для мошенников остается сам человек. Именно несоблюдение необходимых правил и рабочих предписаний зачастую приводят к появлению брешей и проблем в защите информации в Интернете для любой компании. Именно поэтому рекомендуется применять различные организационные методы: Составление четких инструкций, правил и схем работы для персонала, имеющего доступ к информации. Использование электронных ключей, подтверждающих личность сотрудника. Установка сертифицированных программ на рабочие гаджеты. Формулирование конкретных инструкций для службы охраны, включая четкие правила выноса документов с объекта. Использование принципа ответственности за разглашение конфиденциальной информации. Дополнительно подписываются соглашение или строка добавляется в типовый договор. Использование программ, не дающих прямой доступ ко всей информации. Использование систем, предотвращающих случайное или умышленное удаление внесенных данных, а также незаметную администратору корректировку. Ранжирование предоставленной информации для сотрудников разных уровней. Ограничение объема доступных действий. При создании идеальной системы защиты учитывается регулярная проверка действий каждой рабочей единицы. Сотрудникам предоставляется полностью оборудованное рабочее место со всей необходимой аппаратурой, установленным на нее лицензионным программным обеспечением. Также рекомендуется опечатывать корпуса компьютеров и носители информации. Современный рынок позволяет выстроить практически идеальную систему защиты информации в Интернете при использовании методов всех уровней.

Слайд 18.

Проверка самостоятельной работы.

1. Доменные адреса (адрес компьютера в текстовом представлении)
2. Домен верхнего уровня (состоит из двух, трех или четырех букв)
3. Типы доменов верхнего уровня (двухбуквенные, трехбуквенные)
4. Служба доменных имен DNS (преобразовывает доменные адреса в IP – адреса)

Слайд 19.

Пример адрес интернет ресурса записанного в стандарте DNS.

<http://www.myhost.mydomain.spb.ru>

http:// - протокол передачи гипертекстового документа (Hyper Text Transfer Protocol);

www - World Wide Web - Всемирная паутина;

myhost.mydomain - домен третьего уровня;

spb - домен второго уровня;

Ru - домен первого уровня.

Слайд 20. Как вы думаете с помощью какого адреса мы быстрее найдем ответ на поставленный вопрос?

Слайд 21.

Термин

«доменное имя» иногда заменяют английской аббревиатурой URL(UniformResourceLocation – универсальный указатель ресурсов) - адрес конкретного файла (web-страницы).

<http://schools.keldysh.ru/files/index.html>

http – протокол сайта

schools.keldysh.ru – в нашем случае играет роль полного доменного имени, оно пишется в зависимости от названия сайта

/files/ – Путь, который нужно проделать, чтобы найти этот файл. Иными словами – путь к файлу.

index.html – Имеющаяся информация о файле, имя файла.

Слайд 22,23,24

Задача на составление доменного адреса

Слайд 22. ГВЖЕДБА

Слайд 23. ЖВУГАБД

Слайд 24. ДБГЖАВЕ

Слайд 25.

Что мы узнали на уроке.

1. Что такое IP –адрес компьютера.
2. что такое доменное имя компьютера.
3. что такое URL – адрес компьютера

6. Домашнее задание.

Слайд 26.

1. Запишите в тетради IP – адрес вашего домашнего компьютера.
2. Определите, к какому классу адресов он относится

7. Рефлексия. Подведение итогов урока.

ОЦЕНИТЕ ВАШУ ВКЛЮЧЁННОСТЬ В УРОК

1	2	3	4	5	6	7	8	9	10

ВЫБЕРИТЕ ЭМОЦИОНАЛЬНУЮ СОСТАВЛЯЮЩУЮ УРОКА



НАСКОЛЬКО ВЫ ОЦЕНИВАЕТЕ УСВОЕНИЕ ВАМИ ДАННОЙ ИНФОРМАЦИИ

1	2	3	4	5	6	7	8	9	10

(Подведение итога урока. Выставление оценок.)

На уроке мы познакомились с компьютерными сетями, научились просматривать ip-адрес, научились определять адрес сети.

Используемые ресурсы.

- <http://pc-azbuka.ru/chto-takoe-internet/>
- <http://ru.wikipedia.org/wiki/Интернет/>
- <http://ru.wikipedia.org/wiki/Интернет-провайдер>
- <http://www.h20.ru/internet.php>
- <http://likbez-net.ru/kak-rabotaet-internet.html>
- http://speed-tester.info/info_4_chto_takoe_ip_adres_kak_uznat_ip_adres.html
- <http://didaktor.ru/ispolzovanie-shablona-s-makrosom-drag-and-drop/>
- http://shinkarenkoea.ucoz.ru/index/reshenie_zadach_egeh_na_vosstanovlenie_ip_adresa/0-29
- <http://www.myshared.ru/slide/593246/>
- http://u.yablyk.com/2013/11/mobile_internet.jpg
- http://2.bp.blogspot.com/-f2VIg-C7970/T19GwnJfgYI/AAAAAAAAAAM/eDZsS-Fdamk/s1600/-_1~1.JPG

- http://schoobit.ru/wp-content/uploads/2012/01/mozhno_li_zarabativat_v_internete.jpg
 - <http://100facts.ru/wp-content/uploads/2013/10/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82.jpg>
 - <http://img.megaobzor.com/troyan/WEB3.jpg>
 - http://www.sunhome.ru/UsersGallery/wallpapers/258/internet_oboi_dlya_rabochego_stola.jpg
 - http://basik.ru/images/blue_wallpaper/48_blue_wallpaper.jpg
 - <http://u-borisicha.ru/wp-content/uploads/2014/03/what-to-do-on-the-Internet1.jpg>
 - <http://to-name.ru/images/historical-events/computer-engineering/internet-censorship.jpg>
 - <http://aironetsp.ru/images/amatek/logo.jpg>
 - <http://www.novintex.ru/files/1/1350.jpg>
 - <http://support.usr.com/support/5686g/5686g-ug/images/step3.gif>
 - <http://www.h20.ru/images/stories/misc/internet.jpg>
 - <http://kaimi.ru/wp-content/uploads/2011/08/client-server.jpg>
 - <http://www.gigamark.com/images/stories/servers1.jpg>
 - <http://www.skullbox.net/clusters/apple.jpg>
 - <http://pcnotes.ru/wp-content/uploads/2012/03/client-server.png>
 - <http://www.cospec.com.ar/images/Logos%20browser%20Internet.png>
 - <http://www.it59.ru/display6>
 - <http://www.ixbt.com/short/images/2013/Jun/shehre-580x472.jpg>
 - <http://mikro-soft.ru/wp-content/uploads/2014/05/a61d421e9871bdc8ebe35e72013ee4a89.png>
 - <http://iport.kz/uploads/images/00/05/89/2012/03/14/2ee2c7.png>
 - <http://computerkafe.ru/sites/default/files/styles/large/public/field/image/ip-address.jpg?itok=Gu1j4iN3>
- <https://skillbox.ru/media/code/model-tcpip-cto-eto-takoe-i-kak-ona-rabotaet/>
- <https://nsportal.ru/vu/fakultet-informatsionnykh-tekhnologii/osnovy-raboty-s-globalnoy-setyu-internet/lektsiya-4>