ГЛОБАЛЬНАЯ СЕТЬ "ИНТЕРНЕТ"

(модуль III)

ВВЕДЕНИЕ

Интернет (произносится [*интэрнэ́т*]; англ. *Internet*) — всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины (World Wide Web (WWW) и множества других систем (протоколов) передачи данных. Часто упоминается как **Всемирная сеть** и **Глобальная сеть,** в обиходе иногда употребляют сокращённое наименование **Инет.**

В настоящее время, когда слово «Интернет» употребляется в обиходе, чаще всего имеется в виду Всемирная паутина и доступная в ней информация, а не сама физическая сеть.

Уже к середине 2008 года число пользователей, регулярно использующих Интернет, составило около 1,5 млрд человек (около четверти населения Земли). Вместе с подключёнными к нему компьютерами, Интернет служит основой для развития *информационного общества*.

В 2020 году количество интернет-пользователей в мире выросло до 4,54 миллиарда, что на 7% больше прошлогоднего значения (+ 298 миллионов новых пользователей в сравнении с данными на январь 2019 года).

В январе 2020 года в мире насчитывалось 3,80 миллиарда пользователей социальных сетей, аудитория соцмедиа выросла на 9% по сравнению с 2019 годом (это 321 миллион новых пользователей за год).

В России количество интернет-пользователей, по данным Digital 2020, составило 118 миллионов. Это значит, что интернетом пользуется 81% россиян.

При этом численность аудитории социальных сетей в России на начало 2020 года составила 70 миллионов пользователей, то есть 48% от всего населения страны. Цифра за год не изменилась.

Среднестатистический пользователь проводит в интернете 6 часов 43 минуты каждый день. Это на 3 минуты меньше, чем год назад, но по-прежнему составляет более 100 дней на пользователя в год. Если оставить около 8 часов

в сутки на сон, это значит, что сейчас более 40% времени бодрствования мы проводим в интернете.

В совокупности глобальная аудитория интернета будет онлайн 1,25 миллиарда лет за один только 2020 год, и треть этого времени уйдет на социальные сети. Количество времени, которое люди проводят в интернете, сильно отличается в разных странах. Так, на Филиппинах это 9 часов 45 минут в день, а в Японии — 4 часов 22 минуты. **Россияне сидят в интернете 7 часов 17 минут каждый день.**

Сегодня чуть более 40% от общей численности населения мира — примерно 3,2 миллиарда человек — еще не подключены к интернету. Более миллиарда «неподключенных» живут в Южной Азии (31% от общего числа). На страны Африки приходится 27%, то есть 870 миллионов человек по всему континенту.

В этих регионах есть зависимость между уровнем доступа в интернет и возрастом пользователей: в онлайн не выходят более половины населения Африки в возрасте до 20 лет и более 460 миллионов человек в возрасте до 13 лет в Южной Азии.

Имеет значение и пол. По данным Международного союза электросвязи (ITU), женщины реже имеют доступ в интернет, чем мужчины. Гендерный разрыв также наблюдается среди аудитории социальных сетей. Например, сегодня женщины в Южной Азии пользуются социальными сетями в три раза реже по сравнению с мужчинами. Более половины женщин, проживающих в Индии сейчас, вообще не знают о существовании мобильного интернета.

В ООН полагают, что главная причина такого дисбаланса кроется в «глубоко укоренившихся социальных нормах и традициях». Независимо от причины количество «неподключенных» будет в значительной степени зависеть от повышения доступности цифровых технологий сферы для женщин, особенно в развивающихся странах.

На мобильные телефоны теперь приходится больше половины времени, которое мы проводим в интернете — 50,1%.

История Интернет: как все начиналось

В 1957 году Министерство обороны США посчитало, что на случай войны Америке нужна надёжная система передачи информации. Агентство передовых оборонных исследовательских проектов США (DARPA) предложило разработать для этого компьютерную сеть. Разработка такой сети была поручена Калифорнийскому университету в Лос-Анджелесе, Стэнфордскому исследовательскому центру, Университету Юты и Университету штата Калифорния в Санта-Барбаре. Компьютерная сеть

была названа *ARPANET*(англ. *Advanced Research Projects Agency Network*), и в 1969 году в рамках проекта сеть объединила четыре указанных научных учреждения. Все работы финансировались Министерством обороны США. Затем сеть ARPANET начала активно расти и развиваться, её начали использовать учёные из разных областей науки.

Первый сервер ARPANET был установлен 2 сентября 1969 года в Калифорнийском университете в Лос-Анджелесе. Компьютер Honeywell DP-516 имел 24 Кб оперативной памяти.

29 октября 1969 года в 21:00 между двумя первыми узлами сети ARPANET, находящимися на расстоянии в 640 км — в Калифорнийском университете Лос-Анджелеса (UCLA) и в Стэнфордском исследовательском институте (SRI) — провели сеанс связи. Чарли Клайн (Charley Kline) пытался выполнить удалённое подключение к компьютеру в SRI. Успешную передачу каждого введённого символа его коллега Билл Дювалль (Bill Duvall) из SRI подтверждал по телефону.

В первый раз удалось отправить всего три символа «LOG», после чего сеть перестала функционировать. LOG должно было быть словом LOGON (команда входа в систему). В рабочее состояние систему вернули уже к 22:30 и следующая попытка оказалась успешной. Именно эту дату можно считать **Днём рождения Интернета**.

К 1971 году была разработана первая программа для отправки электронной почты по сети. Эта программа сразу стала очень популярна.

В 1973 году к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной.

В 1970-х годах сеть в основном использовалась для пересылки электронной почты, тогда же появились первые списки почтовой рассылки, новостные группы и доски объявлений. Однако в то время сеть ещё не могла легко взаимодействовать с другими сетями, построенными на других технических стандартах. К концу 1970-х годов начали бурно развиваться протоколы передачи данных, которые были стандартизированы в 1982—83 годах. Активную роль в разработке и стандартизации сетевых протоколов играл Джон Постел. 1 января 1983 года сеть ARPANET перешла с протокола NCP на TCP/IP, который успешно применяется до сих пор для объединения (или, как ещё говорят, «наслоения») сетей. Именно в 1983 году термин «Интернет» закрепился за сетью ARPANET.

В 1984 году была разработана система доменных имён (англ. *Domain Name System, DNS*).

В 1984 году у сети ARPANET появился серьёзный соперник: Национальный научный фонд США (NSF) основал обширную межуниверситетскую сеть NSFNet (англ. *National Science Foundation Network*), которая была составлена из более мелких сетей (включая известные тогда сети Usenet и Bitnet) и имела гораздо бóльшую пропускную способность, чем ARPANET. К этой сети за год подключились около 10 тыс. компьютеров, звание «Интернет» начало плавно переходить к *NSFNet*.

В 1988 году был разработан протокол Internet Relay Chat (IRC), благодаря чему в Интернете стало возможно общение в реальном времени (чат).

В 1989 году в Европе, в стенах Европейского совета по ядерным исследованиям (фр. *Conseil Européen pour la Recherche Nucléaire, CERN*) родилась концепция Всемирной паутины. Её предложил знаменитый британский учёный Тим Бернерс-Ли, он же в течение двух лет разработал протокол HTTP, язык HTML и идентификаторы URI.

Соавтор Тима Бернерса-Ли по формулировке целей и задач проекта World Wide Web в CERN, бельгийский исследователь Роберт Каиллиалу (Robert Cailliau) разъяснял позднее его понимание истоков этого проекта:

> История всех великих изобретений, как это давно и хорошо известно, базируется на большом числе им предшествующих. В случае Всемирной паутины (WWW) следовало бы в этом контексте, видимо, отметить по крайней мере два важнейших для успеха проекта пути развития и накопления знаний и технологий: 1) история развития систем типа гипертекста; 2) Интернет-протокол, который собственно и сделал всемирную сеть компьютеров наблюдаемой реальностью.
>
> — Из речи на открытии Европейского отделения W3 Консорциума. Париж. Ноябрь 1995.

В 1990 году сеть ARPANET прекратила своё существование, полностью проиграв конкуренцию NSFNet. В том же году было зафиксировано первое подключение к Интернету по телефонной линии (т. н. «дозво́н» — англ. *Dialup access*).

В 1991 году Всемирная паутина стала общедоступна в Интернете, а в 1993 году появился знаменитый веб-браузер NCSA Mosaic. Всемирная паутина набирала популярность.

> Можно считать что существует две ясно различимые эры в истории Web: [до браузера Mosaic] Марка Андриссена и после. Именно сочетание веб-протокола от Тима Бернерс-Ли, который обеспечивал коммуникацию, и браузера (Mosaic) от Марка Андриссена, который предоставил функционально

совершенный пользовательский интерфейс, создало условия для наблюдаемого взрыва (интереса к Веб). За первые 24 месяца, истекшие после появления браузера Mosaic, Web прошел стадию от полной неизвестности (за пределами считанного числа людей внутри узкой группы ученых и специалистов лишь одного мало кому известного профиля деятельности) до полной и абсолютно везде в мире его распространенности.

— A Brief History of Cyberspace, Mark Pesce, ZDNet, 15 октября 1995

В 1995 году NSFNet вернулась к роли исследовательской сети, маршрутизацией всего трафика Интернета теперь занимались сетевые провайдеры, а не суперкомпьютеры Национального научного фонда.

В том же 1995 году Всемирная паутина стала основным поставщиком информации в Интернете, обогнав по трафику протокол пересылки файлов FTP. Был образован Консорциум всемирной паутины (W3C). Можно сказать, что Всемирная паутина преобразила Интернет и создала его современный облик. С 1996 года Всемирная паутина почти полностью подменяет собой понятие «Интернет».

В 1990-е годы Интернет объединил в себе большинство существовавших тогда сетей (хотя некоторые, как Фидонет, остались обособленными). Объединение выглядело привлекательным благодаря отсутствию единого руководства, а также благодаря открытости технических стандартов Интернета, что делало сети независимыми от бизнеса и конкретных компаний. К 1997 году в Интернете насчитывалось уже около 10 млн компьютеров, было зарегистрировано более 1 млн доменных имён. Интернет стал очень популярным средством для обмена информацией.

В настоящее время подключиться к Интернету можно через спутники связи, радио-каналы, кабельное телевидение, телефон, сотовую связь, специальные оптико-волоконные линии или электропровода. Всемирная сеть стала неотъемлемой частью жизни в развитых и развивающихся странах.

В течение пяти лет Интернет достиг аудитории свыше 50 миллионов пользователей. Другим средствам массовой информации требовалось гораздо больше времени для достижения такой популярности:

Информационная среда	***Время, лет***
Радио	38
Телевидение	13
Кабельное телевидение	10
Интернет	5

С 22 января 2010 года прямой доступ в Интернет получил экипаж Международной космической станции.

Предсказания появления

- Русский писатель, философ и общественный деятель XIX века Владимир Одоевский в незаконченном утопическом романе «4338-й год», написанном в 1837 году, похоже, первым предсказал появление современных блогов и Интернета: в тексте романа есть строки «между знакомыми домами устроены магнетические телеграфы, посредством которых живущие на далёком расстоянии общаются друг с другом».
- Идею применения электрической информационной связи для целей бизнеса упоминал в 1908 году Никола Тесла:

  «Когда проект будет завершён, бизнесмен в Нью-Йорке сможет диктовать указания, и они будут немедленно появляться в его офисе в Лондоне или любом другом месте. Он сможет со своего рабочего места позвонить любому абоненту на планете, не меняя существующего оборудования. Дешёвое устройство, по размерам не больше, чем часы, позволит его обладателю слушать на воде и суше музыку, песни, речи политиков, учёных, проповеди священников, доставляемые на большие расстояния. Таким же образом любое изображение, символ, рисунок, текст могут быть переданы из одного места в другое. Миллионы таких устройств могут контролироваться единственной станцией. И самое главное, что все это будет передаваться без проводов…»

- Английский писатель Эдвард Морган Форстер в фантастической повести-антиутопии «Машина останавливается» (1909) изобразил всемирную автоматическую систему, обслуживающую человечество. Люди становятся полностью зависимы от неё, постепенно деградируют физически и живут почти безвылазно и одиноко в своих квартирах-сотах, общаясь только виртуально. Система даёт сбой и останавливается, все погибают. Предсказана будущая для тогдашнего времени проблема, связанная с Интернетом — далеко зашедшая интернет-зависимость.
- В рассказе Мюррея Лейнстера «Логик по имени Джо» (1946) предсказан современный Интернет и связанные с ним проблемы и опасности. Логики (компьютеры), объединённые в мировую сеть, контролируют банки, телекоммуникации, авиарейсы и многое другое. Бракованный логик Джо по заданию пользователей ищет в сети людей, рецепты изготовления бомбы на дому и т. п.

- Многие писатели-фантасты описывали большие общенациональные или общепланетные компьютеры, которые можно назвать прообразом современных интернет-серверов. Среди них Multivac (*англ.*) (1955—1979), придуманный Айзеком Азимовым, Большой Всепланетный Информаторий (1970—80-е годы) братьев Стругацких, Большая Академическая Машина в романе «Люди как боги» (1966) Сергея Снегова. В этих случаях писатели-фантасты отталкивались от современных им мэйнфреймов, увеличивая их масштабы.

Перспективы

Подобно тому, как коммерческие интернет-провайдеры соединяются посредством точек обмена трафиком, исследовательские сети объединяются в свои подсети, такие как:

- National LambdaRail
- Abilene Network
- GEANT
- GLORIAD

В России наиболее известен проект «Ábилин» (англ. *Abilene Network*) — высокоскоростная экспериментальная сеть, созданная и поддерживаемая американским консорциумом «Интернет2» (англ. *Internet2*). Сам консорциум является некоммерческой организацией и занимается разработкой передовых приложений и сетевых технологий. Его сеть Абилин уже объединяет более 230 американских университетов, научных центров и других учреждений. Особенностью сети Абилин является высокая скорость передачи данных, теоретически она может достигать 10 Гбит/с (OC-192c), реально скорость составляет порядка 6—8 Гбит/с.

Дальнейшее совершенствование общедоступной сети Интернет многие связывают с внедрением концепции семантической паутины, что позволило бы людям и компьютерам более эффективно взаимодействовать в процессе создания, классификации и обработки информации.

Ключевые принципы

Интернет состоит из многих тысяч корпоративных, научных, правительственных и домашних компьютерных сетей. Объединение сетей разной архитектуры и топологии стало возможно благодаря протоколу IP (англ. *Internet Protocol*) и принципу маршрутизации пакетов данных.

Протокол IP был специально создан агностическим в отношении физических каналов связи. То есть любая система (сеть) передачи цифровых данных, проводная или беспроводная, для которой существует стандарт инкапсуляции в неё IP-пакетов, может передавать и трафик Интернета. Агностицизм протокола IP, в частности, означает, что компьютер или маршрутизатор должен знать тип сетей, к которым он непосредственно присоединён, и уметь работать с этими сетями; но не обязан (и в большинстве случаев не может) знать, какие сети находятся за маршрутизаторами.

На стыках сетей специальные маршрутизаторы (программные или аппаратные) занимаются автоматической сортировкой и перенаправлением пакетов данных, исходя из IP-адресов получателей этих пакетов. Протокол IP образует единое адресное пространство в масштабах всего мира, но в каждой отдельной сети может существовать и собственное адресное подпространство, которое выбирается исходя из класса сети. Такая организация IP-адресов позволяет маршрутизаторам однозначно определять дальнейшее направление для каждого пакета данных. В результате между отдельными сетями Интернета не возникает конфликтов, и данные беспрепятственно и точно передаются из сети в сеть по всей планете и ближнему космосу.

Сам протокол IP был рождён в дискуссиях внутри организации IETF (англ. *Internet Engineering Task Force*; Task force — группа специалистов для решения конкретной задачи), чьё название можно вольно перевести как «Группа по решению задач проектирования Интернета». IETF и её рабочие группы по сей день занимаются развитием протоколов Всемирной сети. IETF открыта для публичного участия и обсуждения. Комитеты организации публикуют так называемые документы RFC. В этих документах даются технические спецификации и точные объяснения по многим вопросам. Некоторые документы RFC возводятся организацией IAB(англ. *Internet Architecture Board* — Совет по архитектуре Интернета) в статус стандартов Интернета (англ. *Internet Standard*). С 1992 года IETF, IAB и ряд других интернет-организаций входят в Общество Интернета (англ. *Internet Society*, *ISOC*). Общество Интернета предоставляет организационную основу для разных исследовательских и консультативных групп, занимающихся развитием Интернета.

Языки

Свобода доступа пользователей Интернета к информационным ресурсам не ограничивается государственными границами и/или национальными доменами, но языковые границы сохраняются. Преобладающим языком Интернета является английский язык. Вторым по популярности

является китайский язык, а третьим — испанский. Русский язык занимает 9 место.

Язык является одним из часто используемых признаков деления Интернета, наряду с делением по государствам, регионам и доменам первого уровня. Название языковых сфер Интернета даётся по названию используемого языка. Русскоязычная сфера Интернета получила название «Русский Интернет», сокращённо Рунет.

Рунет

Рунет (с прописной буквы, читается [*рунэ́т*]) — русскоязычная часть всемирной сети Интернет. Более узкое определение гласит, что Рунет — это часть Всемирной паутины, принадлежащая к национальным доменам .su, .ru и .рф. 1987—94 годы стали ключевыми в зарождении русскоязычного Интернета. 28 августа 1990 года профессиональная научная сеть, выросшая в недрах Института атомной энергии им. И. В. Курчатова и ИПК Минавтопрома и объединившая учёных-физиков и программистов, соединилась с мировой сетью Интернет, положив начало современным российским сетям. 19 сентября 1990 года был зарегистрирован домен первого уровня .su в базе данных Международного информационного центра InterNIC. В результате этого Советский Союз стал доступен через Интернет. **7 апреля 1994 года** в InterNIC был зарегистрирован российский домен .ru.

Домен «.рф» (punycode: xn--p1ai; **Р**оссийская **Ф**едерация), позволяющий использовать в адресе URL кириллические символы, делегирован в корневой зоне DNS 12 мая 2010 года около 17:20 по московскому времени. По статистике Технического центра «Интернет», на конец 2010 года в зоне .рф зарегистрировано около 700 000 доменов, около 350 000 из них делегировано. По данным Координационного центра национального домена сети Интернет, из доменных имен в зоне .рф, зарегистрированных к настоящему времени, только 8 % представляют собой общеупотребительные слова русского языка. Еще 30 % образованы несколькими словами, все остальные домены представляют собой имена людей, литературных персонажей, названий компаний. Подавляющее большинство имен принадлежит владельцам товарных знаков. Почти половина имен была зарегистрирована в Москве, еще 9 % — в Московской области, 8 % — в Санкт-Петербурге.

Браузеры

Браузер — компьютерная программа для просмотра веб-страниц. Существует довольно много браузеров. Самые популярные из них — это Google Chrome, Yandex, Mozilla Firefox, Internet Explorer, Opera, Safari.

Протоколы

Протокол в данном случае — это, образно говоря, «язык», используемый компьютерами для обмена данными при работе в сети. Чтобы различные компьютеры сети могли взаимодействовать, они должны «разговаривать» на одном «языке», то есть использовать один и тот же протокол. Проще говоря, протокол — это правила передачи данных между узлами компьютерной сети. Систему протоколов Интернет называют «стеком протоколов TCP/IP».

Наиболее распространённые интернет-протоколы (в алфавитном порядке, сгруппированные в примерном соответствии модели OSI):

Уровень OSI	***Протоколы, примерно соответствующие уровню OSI***
Прикладной	BGP, DNS, FTP, HTTP, HTTPS, IMAP, LDAP, POP3, SNMP , SMTP, SSH, Telnet, XMPP (Jabber)
Сеансовый/Представления	SSL, TLS
Транспортный	TCP, UDP
Сетевой	EIGRP, ICMP, IGMP, IP, IS-IS, OSPF, RIP
Канальный	Arcnet, ATM, Ethernet, Frame relay, HDLC, PPP, L2TP, SLIP, Token ring

Есть ещё целый ряд протоколов, ещё не стандартизированных, но уже очень популярных в Интернете:

- OSCAR
- CDDB
- MFTP (сеть eDonkey2000)
- BitTorrent
- Gnutella

Эти протоколы в большинстве своём нужны для обмена файлами и текстовыми сообщениями, на некоторых из них построены целые файлообменные сети.

Сервисы

В настоящее время в Интернете существует достаточно большое количество сервисов, обеспечивающих работу со всем спектром ресурсов. Наиболее известными среди них являются:

- электронная почта (E-mail), обеспечивающая возможность обмена сообщениями одного человека с одним или несколькими абонентами;
- телеконференции, или группы новостей (Usenet), обеспечивающие возможность коллективного обмена сообщениями;

- сервис FTP — система файловых архивов, обеспечивающая хранение и пересылку файлов различных типов;
- сервис Telnet, предназначенный для управления удаленными компьютерами в терминальном режиме;
- World Wide Web (WWW, W3) — гипертекстовая (гипермедиа) система, предназначенная для интеграции различных сетевых ресурсов в единое информационное пространство;
- сервис DNS, или система доменных имен, обеспечивающий возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов;
- сервис IRC, предназначенный для поддержки текстового общения в реальном времени (chat);
- потоковое мультимедиа.

Перечисленные выше сервисы относятся к стандартным. Это означает, что принципы построения клиентского и серверного программного обеспечения, а также протоколы взаимодействия сформулированы в виде международных стандартов. Следовательно, разработчики программного обеспечения при практической реализации обязаны выдерживать общие технические требования.

Наряду со стандартными сервисами существуют и нестандартные, представляющие собой оригинальную разработку той или иной компании. В качестве примера можно привести различные системы типа Instant Messenger (своеобразные интернет-пейджеры — ICQ, AOl, Demos on-line и т. п.), системы интернет-телефонии, трансляции радио и видео и т. д. Важной особенностью таких систем является отсутствие международных стандартов, что может привести к возникновению технических конфликтов с другими подобными сервисами.

Для стандартных сервисов также стандартизируется и интерфейс взаимодействия с протоколами транспортного уровня. В частности, за каждым программным сервером резервируются стандартные номера TCP- и UDP-портов, которые остаются неизменными независимо от особенностей той или иной фирменной реализации как компонентов сервиса, так и транспортных протоколов. Номера портов клиентского программного обеспечения так жестко не регламентируются. Это объясняется следующими факторами:

- во-первых, на пользовательском узле может функционировать несколько копий клиентской программы, и каждая из них должна

однозначно идентифицироваться транспортным протоколом, то есть за каждой копией должен быть закреплен свой уникальный номер порта;

- во-вторых, клиенту важна регламентация портов сервера, чтобы знать, куда направлять запрос, а сервер сможет ответить клиенту, узнав адрес из поступившего запроса.

Услуги

Сейчас наиболее популярные услуги Интернета — это:

- Всемирная паутина
  - Веб-форумы
  - Блоги
  - Вики-проекты (и, в частности, Википедия)
  - Интернет-магазины
  - Интернет-аукционы
  - Социальные сети
- Электронная почта и списки рассылки
- Группы новостей (в основном, Usenet)
- Файлообменные сети
- Электронные платёжные системы
- Интернет-радио
- Интернет-телевидение
- IP-телефония
- Мессенджеры
- FTP-серверы
- IRC (реализовано также как веб-чаты)
- Поисковые системы
- Интернет-реклама
- Удалённые терминалы
- Удалённое управление
- Многопользовательские игры
- Web 2.0

Юридические аспекты и общие свойства

1. У Интернета нет собственника, так как он является совокупностью сетей, которые имеют различную географическую принадлежность.
2. Интернет нельзя выключить целиком, поскольку маршрутизаторы сетей не имеют единого внешнего управления.
3. Интернет стал достоянием всего человечества.
4. У Интернета имеется много полезных и вредных свойств, эксплуатируемых заинтересованными лицами.
5. Интернет, прежде всего, средство открытого хранения и распространения информации. По маршруту транспортировки незашифрованная информация может быть перехвачена и прочитана.
6. Интернет может связать каждый компьютер с любым другим, подключённым к Сети, так же, как и телефонная сеть. Если телефон имеет автоответчик, он способен распространять информацию, записанную в него, любому позвонившему.

7. Сайты в Интернете распространяют информацию по такому же принципу, то есть индивидуально, по инициативе читателя.
8. Спам-серверы и «зомби-сети» распространяют информацию по инициативе отправителя и забивают почтовые ящики пользователей электронной почты спамом точно так же, как забивают реальные почтовые ящики распространители рекламных листовок и брошюр.
9. Распространение информации в Интернете имеет ту же природу, что и слухи в социальной среде. Если к информации есть большой интерес, она распространяется быстро и широко, нет интереса — нет распространения.
10. Чтение информации, полученной из Интернета или любой другой сети ЭВМ, относится, как правило, к непубличному воспроизведению произведения. За распространение информации в Интернете (разглашение), если это государственная или иная тайна, клевета, другие запрещённые законом к распространению сведения, вполне возможна юридическая ответственность по законам того места, откуда информация введена.
11. 3 июня 2011 года была принята резолюция ООН, признающая доступ в Интернет *базовым правом человека*. Отключение конкретных регионов от Интернета с июня 2011 года считается нарушением прав человека.

Цензура

Во многих странах существуют серьёзные ограничения на функционирование сети, то есть на государственном уровне осуществляется запрет на доступ к отдельным сайтам (СМИ, аналитическим, порнографическим) или ко всей сети. Одним из примеров может служить реализованный в КНР проект «Золотой щит» — система фильтрации трафика на интернет-канале между провайдерами и международными сетями передачи информации.

Поскольку в Интернете присутствуют информационные ресурсы, которые бывают неудобны для некоторых правительств, то последние пытаются декларировать Интернет как средство массовой информации, со всеми вытекающими ограничениями. Но на самом деле, Интернет — это только носитель, информационная среда, как и телефонная сеть или просто бумага. В мире встречается и государственная монополия на само подключение к сети Интернет.

Поскольку Интернет сначала развивался стихийно, то только на этапе превращения его в глобальную сеть государства стали проявлять интерес к его функционированию. Пока возможности цензуры ограничены, так как ещё ни одно государство в мире не решилось полностью отключить внутренние сети от внешних. По признанию одного из отцов Интернета[*кто?*], «мы не смогли бы

сделать ничего подобного, если бы это с самого начала находилось под контролем государства».

В то же время многие информационные ресурсы официально подвергают цензуре (модерации) публикуемую ими информацию в зависимости от проводимой политики и собственных внутренних правил. Это не противоречит демократическим принципам свободы слова.

От нежелательного контента можно защититься установкой фильтров на компьютере пользователя.

«Самый эффективный метод цензуры в Интернете — это работа с провайдерами. Можно ввести список адресов, которые будут недоступны пользователям».

Для преодоления цензуры в Интернете пользователи используют возможность доступа к заблокированным ресурсам через другие, разрешённые ресурсы. Таковыми могут выступать веб-прокси и прокси-серверы, анонимайзеры и анонимные сети, RSS-агрегаторы, веб-сервисы перевода содержимого веб-страниц по указанию адреса страницы (например, Google Translate), виртуальные частные сети.

Субкультуры

Современный Интернет имеет также очень много социальных и культурных граней. Он является универсальной глобальной информационной средой.

Интернет-сообщества

Интернет предоставляет широчайшие технические возможности для общения. Кроме того, в Интернете сравнительно легко найти людей со схожими интересами и взглядами на мир, или найти прошлых знакомых, которые в силу жизненных обстоятельств были разбросаны по всей Земле. Вдобавок, общение в Сети начать психологически проще, чем при личной встрече. Эти причины обусловливают создание и активное развитие веб-сообществ — групп людей, имеющих общие интересы и общающихся преимущественно через Интернет. Подобные интернет-сообщества постепенно начинают играть ощутимую роль в жизни всего общества.

Интернет-зависимость

С возрастанием популярности Интернета проявились и негативные аспекты его применения. В частности, некоторые люди настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Психологическую в своей основе, интернет-зависимость сравнивают с наркоманией —

физиологической зависимостью от наркотических веществ, где также присутствует психический компонент. Интернет-зависимость определяется как навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в стране таковых 4—6 %.

Киберпанк

Интернет, киберпространство и виртуальная реальность нашли своё отражение и в современном искусстве. Ещё в середине 1980-х годов сформировался особый поджанр научной фантастики, фокусирующийся на компьютерах, высоких технологиях и проблемах, возникающих в обществе в связи с губительным применением плодов технического прогресса. Сюжетом произведений этого жанра часто становится борьба хакеров с могущественными корпорациями.

Жанр получил широкое распространение в литературе, кинематографе, альтернативной музыке, графических произведениях (особенно аниме) и в компьютерных играх. Сам термин *киберпанк* придуман и введён в употребление писателем Брюсом Бетке, который в 1983 году опубликовал одноимённый рассказ. Меньшее распространение имеют такие ответвления жанра, как кибертрэш и нанопанк.

Троллинг

Троллинг — психологическое и социальное явление, развившееся в Интернете в 1990-х годах и зачастую мешающее нормальному общению в Сети. Интернет-троллями или просто троллями (англ. *troll*) во Всемирной сети называют людей, которые намеренно публикуют провокационные сообщения и статьи (на Форумах, в группах новостей Usenet, в вики-проектах), т. н. «вброс», призванные разжечь конфликты между их участниками, вызвать флейм, оскорбления и так далее. Сами подобные статьи и сообщения также иногда называют троллями. Процесс написания таких сообщений и называется *троллингом*.

Буллинг (травля). Тра́вля (бу́ллинг — англ. *bullying*) — агрессивное преследование одного из членов коллектива (особенно коллектива школьников и студентов, но также и коллег) со стороны другого, но также часто группы лиц, не обязательно из одного формального или признаваемого другими коллектива. Травлю организует один (лидер), иногда с сообщниками, а большинство остаются свидетелями. При травле жертва оказывается не в состоянии защитить себя от нападок, таким образом, травля отличается от

конфликта, где силы сторон примерно равны. Травля может быть и в физической, и в психологической форме. Проявляется во всех возрастных и социальных группах. В сложных случаях может принять некоторые черты групповой преступности.

В качестве особой формы травли выделяют групповую травлю («травля толпы»), большинством или всеми членами коллектива (микрособщества), часто начальником, работодателем (жарг. «моббинг»).

Как проявления травли специалисты расценивают оскорбления, угрозы, физическую агрессию, постоянную негативную оценку жертвы и её деятельности, отказ в доверии и делегировании полномочий и так далее.

Угрозы «Интернет»: вирусы

(вредоносные программы)

Компьютерный **вирус** — вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по разнообразным каналам связи. Основная цель вируса — его распространение.

Для защиты от вирусов используют три группы методов:

1. Методы, основанные на *анализе содержимого файлов* (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.
2. Методы, основанные на *отслеживании поведения программ* при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции.
3. Методы *регламентации порядка работы* с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности.

Метод сканирования сигнатур (сигнатурный анализ, сигнатурный метод) основан на поиске в файлах уникальной последовательности байтов — **сигнатуры**, характерной для определенного вируса. Для каждого вновь обнаруженного вируса специалистами антивирусной лаборатории выполняется анализ кода, на основании которого определяется его сигнатура. Полученный кодовый фрагмент помещают в специальную базу данных вирусных сигнатур, с которой работает антивирусная программа. Достоинством данного метода является относительно низкая доля ложных

срабатываний, а главным недостатком — принципиальная невозможность обнаружения в системе нового вируса, для которого отсутствует сигнатура в базе данных антивирусной программы, поэтому требуется своевременная актуализация базы данных сигнатур.

Метод контроля целостности основывается на том, что любое неожиданное и беспричинное изменение данных на диске является подозрительным событием, требующим особого внимания антивирусной системы. Вирус обязательно оставляет свидетельства своего пребывания (изменение данных существующих (особенно системных или исполняемых) файлов, появление новых исполняемых файлов и т. д.). Факт изменения данных — *нарушение целостности* — легко устанавливается путем сравнения контрольной суммы (дайджеста), заранее подсчитанной для исходного состояния тестируемого кода, и контрольной суммы (дайджеста) текущего состояния тестируемого кода. Если они не совпадают, значит, целостность нарушена и имеются все основания провести для этого кода дополнительную проверку, например, путем сканирования вирусных сигнатур. Указанный метод работает быстрее метода сканирования сигнатур, поскольку подсчет контрольных сумм требует меньше вычислений, чем операции побайтового сравнения кодовых фрагментов, кроме того он позволяет обнаруживать следы деятельности любых, в том числе неизвестных, вирусов, для которых в базе данных еще нет сигнатур.

Метод сканирования подозрительных команд (эвристическое сканирование, эвристический метод) основан на выявлении в сканируемом файле некоторого числа подозрительных команд и(или) признаков подозрительных кодовых последовательностей (например, команда форматирования жесткого диска или функция внедрения в выполняющийся процесс или исполняемый код). После этого делается предположение о вредоносной сущности файла и предпринимаются дополнительные действия по его проверке. Этот метод обладает хорошим быстродействием, но довольно часто он не способен выявлять новые вирусы

Метод отслеживания поведения программ принципиально отличается от методов сканирования содержимого файлов, упомянутых ранее. Этот метод основан на анализе поведения запущенных программ, сравнимый с поимкой преступника «за руку» на месте преступления. Антивирусные средства данного типа часто требуют активного участия пользователя, призванного принимать решения в ответ на многочисленные предупреждения системы, значительная часть которых может оказаться впоследствии ложными тревогами. Частота ложных срабатываний (подозрение на вирус для безвредного файла или пропуск вредоносного файла) при превышении

определенного порога делает этот метод неэффективным, а пользователь может перестать реагировать на предупреждения или выбрать оптимистическую стратегию (разрешать все действия всем запускаемым программам или отключить данную функцию антивирусного средства). При использовании антивирусных систем, анализирующих поведение программ, всегда существует риск выполнения команд вирусного кода, способных нанести ущерб защищаемому компьютеру или сети. Для устранения подобного недостатка позднее был разработан метод эмуляции (имитации), позволяющий запускать тестируемую программу в искусственно созданной (виртуальной) среде, которую часто называют песочницей (sandbox), без опасности повреждения информационного окружения. Использование методов анализа поведения программ показало их высокую эффективность при обнаружении как известных, так и неизвестных вредоносных программ.

Антивирусная программа (антивирус, средство антивирусной защиты, средство обнаружения вредоносных программ) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Наиболее известные программы борьбы с компьютерными вирусами:

1. Платные (лицензионные) продукты:

• Антивирус Касперского
• ESET NOD32 Antivirus
• Emsisoft Anti-Malware
• McAfee AntiVirus Plus
• Avira Antivirus Pro
• Webroot SecureAnywhere AntiVirus
• Norton AntiVirus Plus
• Advanced SystemCare Ultimate (с Антивирусом)
• Bitdefender Antivirus Plus
• Malwarebytes Premium

2. Бесплатные продукты:

• Avast Free Antivirus
• Comodo Internet Security Premium
• Avira Free Antivirus
• AVG AntiVirus FREE
• Антивирус Kaspersky Free

- 360 Total Security
- Panda Free Antivirus
- Microsoft Security Essentials
- 360 Total Security Essential
- Bitdefender Antivirus Free Edition

Правила поведения и работы в сети «Интернет»

1. Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей. Письма со сканами документов лучше удалять сразу после отправки или получения, не надо хранить их в почте.
2. Если заходите в соцсеть или почту с чужого компьютера, не забудьте разлогиниться (удалить свои данные для входа; снять «галочку» запоминания).
3. Выключайте Wi-Fi, когда им не пользуетесь. И себя защитите, и заряд батареи сэкономите. Обязательно отключите функцию автоматического подключения к Wi-Fi в вашем телефоне или планшете.
4. Не доверяйте непроверенным Wi-Fi-соединениям, которые не запрашивают пароль. Чаще всего именно такие сети злоумышленники используют для воровства личных данных пользователей.
5. Не заходите в онлайн-банки и другие важные сервисы через открытые Wi-Fi-сети в кафе или на улице. Воспользуйтесь мобильным интернетом.
6. Помните: банки, сервисы и магазины никогда не рассылают писем с просьбой перейти по ссылке, изменить свой пароль, ввести номер банковской карты и секретный код подтверждения или сообщить другие личные данные!
7. Отключите SIRI (голосовой помощник в экосистеме Apple) на айфоне. Скорее всего, вы ей не пользуетесь, а вот мошенники уже научились выводить деньги через интернет-банк голосовыми командами.
8. Заведите несколько адресов электронной почты: личная, рабочая и развлекательная (для подписок и сервисов).
9. Придумайте сложный пароль, для каждого ящика разный.
10. Регулярно меняйте пароли, обновляйте браузер и спам-фильтры.
11. Установите и обновляйте антивирусные программы. Устаревшие версии не могут гарантировать защиту от вредоносного ПО. Ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу нужно как можно чаще получать информацию о методах борьбы с ними.
12. Кликать по ссылкам, пришедшим в сообщениях от незнакомых людей — верный способ попасться на удочку кибермошенников и заразить свое устройство вирусами. Опасная ссылка может прийти и от взломанного

знакомого, поэтому лучше уточните, что такое он вам прислал и нужно ли это открывать.
13. Не запускайте неизвестные файлы, особенно с расширением .exe
14. Внимательно проверяйте адреса ссылок, логотипы, текст и отправителя сообщений.
15. Никогда не отвечайте на спам.
16. Если вам в мессенджер пришла просьба от знакомого с просьбой срочно выслать денег, ничего не отправляйте! Сначала перезвоните ему и удостоверьтесь, что аккаунт не был взломан злоумышленниками.
17. Прочитайте книгу Кевина Митника «Искусство обмана». Митник — культовая фигура в среде информационной безопасности, его книга, как и история жизни, одновременно увлекательна и поучительна. Вы узнаете, как киберпреступники втираются в доверие к людям, манипулируя их чувствами.
18. Минимум личной информации: не публикуйте в сети домашний адрес, не пишите, в какое время вас не бывает дома, не описывайте свой постоянный маршрут, не хвалитесь крупными покупками и вообще постарайтесь не афишировать уровень достатка.
19. Регулярно выполняйте резервное копирование данных. Следуйте правилу «3-2-1»: создайте одну основную копию и две резервные. Сохраните две копии на разных физических носителях, а одну — в облачном хранилище (Google Диск, Яндекс.Диск, специальные решения от Акронис). Не забывайте бэкапить все устройства: смартфоны, планшеты, компьютеры/ноутбуки.
20. Чтобы никогда не терять деньги на незаметных платежах, не покупать дополнительных услуг по ошибке и точно заплатить за нужные, всегда читайте правила перед тем, как поставить галочку напротив чекбокса «согласен» и перейти к оплате.
21. Если в секретном вопросе вы указали девичью фамилию матери, которая сейчас есть в открытом доступе на ее страницах в соцсетях, обязательно поменяйте секретный вопрос.
22. Установите безопасный режим для ребенка. Для этого создайте отдельную учетную запись на сайте выбранной вами поисковой системы или используйте детские поисковики: Гогуль или Спутник.дети.
23. Говорите с ребенком об интернете: договоритесь, чтобы он сообщал вам о найденной нежелательной информации. Объясните, что не вся информация в сети достоверна, и приучите советоваться с вами по любому непонятному вопросу.
24. Не скачивайте сомнительные приложения и не пытайтесь это делать по неизвестным ссылкам. Пользуйтесь только официальными магазинами App Store, Google Play и Windows Market.

25. Совет для пользователей Google Chrome, Firefox и Opera: если вы часто путешествуете и выходите в сеть с ноутбука в общественных местах, установите специальное расширение для браузера для безопасного выхода в интернет. Рекомендуем HTTPS Everywhere от Electronic Frontier Foundation (EFF). По умолчанию этот плагин обеспечивает безопасное соединение для Yahoo, eBay, Amazon и некоторых других веб-ресурсов. Вы также можете добавить сайты по вашему выбору.
26. Постарайтесь ничего не покупать в социальных сетях, особенно с предоплатой. Мы вообще не рекомендуем переводить деньги на карту физических лиц (то есть, когда кто-то просто дает вам номер или реквизиты своей карты).
27. Покупая в интернет-магазинах, сохраняйте здоровый скептицизм. Помните: цена не может быть слишком низкой, тем более, если вы рассчитываете приобрести оригинальную продукцию бренда.
28. Изучите историю магазина в сети, проверьте наличие контактов, выясните, можно ли туда приехать и познакомиться вживую. Читая отзывы, обратите внимание, чтобы они были разными. Заказные отзывы пишут люди, которым приходится делать это много раз в день, поэтому такие тексты будто написаны по шаблону.
29. Посмотрите, как на отзывы реагируют продавцы. Обратите особое внимание на негативные: если их отрабатывают, это хороший знак (причем ситуация должна быть конкретная, содержать номер заказа и т.п.).
30. Платите безопасно! Классический случай — вас переадресуют на защищенную страницу (адрес начинается с «https://»). Если нет, лучше не рисковать. По правилам эквайринга на сайте продавца должна быть информация о том, кто принимает платеж. Прочтите ее и сверьте с тем, что написано на следующей странице.
31. Заведите отдельную (можно виртуальную) карту для платежей в интернете.
32. Если для оплаты в интернете вы пользуетесь своей обычной картой, не храните на ней крупные суммы денег.
33. Подключите в своем банке СМС-информирование о всех операциях по картам и счетам. Так вы сможете быстро заметить, если ваша карта будет скомпрометирована, и заблокировать ее.
34. Страницы ввода конфиденциальной информации любого серьезного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зеленого цвета.
35. Куда обращаться, если что-то пошло не так? Деятельность интернет-магазинов контролируется теми же организациями, что и обычных:

Роспотребнадзором, Обществом защиты прав потребителей. Обязательно напишите на Горячую линию Рунета: www.hotline.rocit.ru

36. Будьте осторожны при общении в сети с незнакомыми, они могут оказаться не теми, за кого себя выдают.

37. Халявы, случайных многомиллионных наследств и неизвестных богатых родственников, которые просто так хотят поделиться, не бывает.

38. Не делайте репостов жалостливых объявлений про милого котика, который срочно ищет дом (а в посте — телефон владельца или номер карты, куда можно перечислить деньги на содержание животного). Велика вероятность, что это мошенники, решившие заработать на сердобольных и доверчивых гражданах.

39. Логотип известного благотворительного фонда еще не означает, что деньги пойдут туда — реквизиты счета могут быть подделаны. Если хотите помогать людям, делайте это только для лично знакомых или, например, с проектом dobro.mail.ru.

40. Не покупайте авиабилеты на незнакомых сайтах, особенно если они стоят гораздо дешевле, чем на всех остальных. Зайдите на настоящийбилет.рф и удостоверьтесь в подлинности ресурса. Также не лишним будет посетить сайт авиакомпании, которой вы хотите улететь, и сравнить цену билета на нужное направление.

41. Обращайте внимание на адрес страницы, где вы оказались: если он отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), введите его вручную самостоятельно.

42. Если на смартфоне появилась надпись «Вставьте сим-карту», срочно зайдите в ближайший офис вашего мобильного оператора или позвоните ему с другого телефона и выясните, в чем проблема. Возможно, кто-то получил дубликат вашей симки и ее нужно срочно заблокировать.

43. По ссылке http://www.tcinet.ru/whois/ можно узнать, когда был создан сайт. Злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают.

44. Потеряли телефон, к которому привязана банковская карта? Срочно блокируйте и симку, и карту.

45. Лучше не пользоваться торрентами: если вы скачиваете нелегальный контент, вы не только обкрадываете любимого автора, но и можете загрузить зараженный вирусом файл.

46. Мошенники создают сайты, на которых вы якобы можете бесплатно посмотреть или скачать приглянувшийся фильм, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров.

47. Для некоторых приложений и сервисов предусмотрен бесплатный тестовый период (например, на 2-3 месяца), после чего вы должны самостоятельно отключить услугу. Если вы этого не сделаете, подписка может быть автоматически продлена и станет платной, а с указанной при регистрации карты начнут списывать деньги.
48. Не участвуйте в акциях с призами, где надо что-то оплатить, а потом попросить сделать то же самое еще нескольких людей. Это пирамида!
49. Всегда блокируйте экран компьютера, даже если отходите «всего на минуточку».
50. Внимательно относитесь ко всем незнакомым интернет-адресам.

Интересные факты

- В начале 21 века эскимосы познакомились с Интернетом, и этот термин понадобилось перевести на их язык. Эксперты выбрали слово '*ikiaqqivik*' — «путешествие сквозь слои». Раньше это слово употреблялось для описания действий шамана, который для поиска ответа на какой-либо вопрос «путешествовал» сквозь время и пространство.
- Неофициальным покровителем Интернета от католический церкви считается Исидор Севильский.
- В 2011 году в Санкт-Петербурге установили памятник Интернету. Данная скульптурная композиция будет представлять из себя уличную скамейку в виде аббревиатуры WWW с бесплатным доступом в Сеть.