Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тихоокеанский государственный университет»

В. В. Стригунов

ВВЕДЕНИЕ В КОМПЬЮТЕРНЫЕ СЕТИ

Утверждено издательско-библиотечным советом университета
в качестве учебного пособия

Хабаровск
Издательство ТОГУ
2016

УДК 004.7(075)
ББК 3971.35я7
С851

Рецензенты: кафедра «Информационные технологии и системы» (ФГБОУ ВПО «Дальневосточный государственный университет путей сообщения» г. Хабаровск); кандидат технических наук, доцент А. Н. Вишневский (ФГБОУ ВПО «Хабаровская государственная академия экономики и права»)
Научный редактор кандидат физико-математических наук, доцент Э. М. Вихтенко

Стригунов, В. В.

С851 Введение в компьютерные сети : учеб. пособие / В. В. Стригунов ; [науч. ред. Э. М. Вихтенко]. – Хабаровск : Изд-во Тихоокеан. гос. ун-та, 2016. – 103 с.

ISBN 978-5-7389-1860-5

В учебном пособии изложены основные принципы построения и функционирования локальных и глобальных компьютерных сетей, а также принципы взаимодействия устройств сети, работы популярных сетевых сервисов, таких как всемирная паутина WWW и электронная почта, рассмотрены вопросы сетевой безопасности. Теоретический материал подкреплен контрольными заданиями.

Для обучающихся по всем направлениям подготовки бакалавриата и специалитета, которые изучают дисциплину «Информатика».

УДК 004.7(075)
ББК 3971.35я7

ISBN 978-5-7389-1860-5

Оглавление

Введение

Компьютеры и компьютерные сети – важная часть сегодняшнего мира, а область их применения охватывает буквально все сферы человеческой деятельности. Последние два десятилетия характеризуются динамичным развитием сетевых технологий. Это связано с широкой популярностью, пришедшей к Интернету, развитием веб-технологий, электронной почты, потокового аудио и видео, систем обмена сообщениями в реальном времени и т. п.

Повсеместное использование компьютерных сетей требует от современного пользователя наличия соответствующих знаний и навыков. Важное значение в приобретении этих знаний имеет раздел «Компьютерные сети» общего учебного курса дисциплины «Информатика». Сам учебный предмет «Компьютерные сети», включающий в себя множество концепций и технологий, является достаточно сложным и запутанным для новичка. Кроме того, профессиональная литература, целиком посвященная компьютерным сетям, слишком избыточна и сложна для понимания студентами непрофильных специальностей и направлений, а также не совсем удобна преподавателям при подготовке к занятиям в рамках курса информатики, содержащего только краткую вводную информацию по компьютерным сетям.

В данном учебном пособии предпринята попытка компактного изложения основ технологий компьютерных сетей без углубления в детали, объяснения общеупотребительных в настоящее время терминов и определений, связанных с функционированием компьютерных сетей.

Порядок изложения материала в пособии следующий: вначале дается общее описание сетевых компьютерных технологий, основы построения и функционирования локальных и глобальных компьютерных сетей, принципы взаимодействия устройств сети, приводятся наиболее важные термины и определения, далее рассматриваются популярные сетевые службы и серви-

сы, такие как всемирная паутина WWW, служба передачи файлов FTP, электронная почта, служба трансляции имен и облачные сервисы. Заключительная теоретическая часть посвящена вопросам сетевой безопасности: безопасному сетевому взаимодействию, разновидности сетевых атак, основам шифрования данных и цифровой подписи, типам вредоносного программного обеспечения.

В довершение с целью закрепления изложенного в пособии материала приведены контрольные задания, включающие три лабораторные работы, и тесты. Лабораторные работы содержат подробное описание заданий и посвящены вопросам адресации компьютеров и ресурсов в сети Интернет, применению инструментов операционной системы Windows при работе с компьютерной сетью, а также использованию некоторых облачных приложений из пакета Google Apps. Тесты можно использовать при подготовке к интернет-экзамену.

Завершает пособие приложение, в котором предлагается список интересных и полезных ресурсов сети Интернет по теме «Компьютерные сети».

1. Общие принципы построения компьютерных сетей

1.1. Компьютерные сети и разделяемые ресурсы

Компьютерные сети, называемые также сетями передачи данных, появились в конце 1960-х гг., и являются результатом развития компьютерных и телекоммуникационных технологий.

Компьютерная сеть образуется при физическом соединении (проводном или беспроводном) двух или более компьютеров для передачи данных между ними. Главной целью объединения вычислительных устройств в сеть является удаленный доступ к ***разделяемым ресурсам***: пользователи компьютеров, подключенных к сети, или приложения, выполняемые на этих компьютерах, получают возможность доступа к разнообразным ресурсам других компьютеров сети, находящихся на расстоянии. К таким разделяемым ресурсам относятся: периферийные устройства (принтеры, плоттеры, сканеры и др.); данные, хранящиеся в оперативной памяти или на внешних запоминающих устройствах; вычислительная мощность (за счет удаленного запуска своих программ на чужих компьютерах).

На те компьютеры, ресурсы которых должны быть доступны всем пользователям сети, устанавливаются программные модули, которые постоянно находятся в режиме ожидания запросов, поступающих по сети от других компьютеров. Такие модули называются программными ***серверами*** (англ. server от serve – служить, обслуживать), так как их главная задача обслуживать запросы на доступ к ресурсам своего компьютера (рис. 1.1).

На компьютерах, пользователи которых хотят получать доступ к ресурсам других компьютеров, также устанавливаются программные модули, которые вырабатывают запросы на доступ к удаленным ресурсам и передают их по сети на нужный компьютер. Такие модули называют программными ***клиентами*** (англ. client).

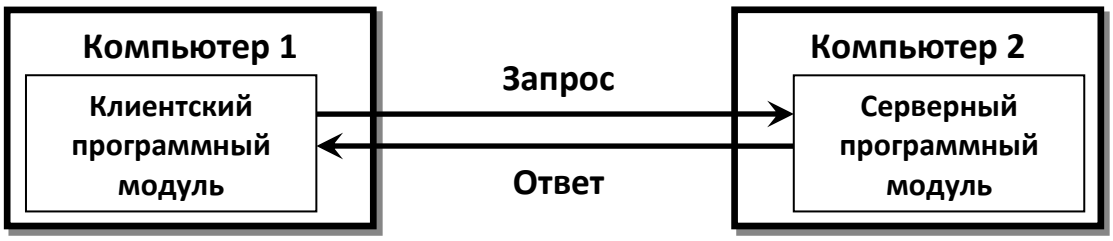


Рис. 1.1. Схема взаимодействия компьютеров

Понятия «клиент» и «сервер» используются не только для обозначения программных модулей, но и самих компьютеров и вычислительных устройств, подключенных к сети. Если компьютер предоставляет свои ресурсы другим компьютерам сети, то он называется сервером, а если он их потребляет – клиентом. Один и тот же компьютер может одновременно играть роли и сервера, и клиента.

В терминах Интернет-технологий компьютеры (клиенты и серверы) подключенные к Интернету называют ***конечными узлами*** или ***хостами***. Они могут представлять собой самые разнообразные вычислительные устройства, различающиеся размерами, вычислительной мощностью и функциональным назначением: персональные компьютеры, ноутбуки, мэйнфреймы, телефоны, смартфоны и др.

1.2. Классификация компьютерных сетей

Компьютерные сети классифицируются по различным признакам. Например, по используемой среде передачи данных (подробно рассматривается в параграфе «Линии связи») различают проводные и беспроводные сети, по скорости передачи данных – низкоскоростные, среднескоростные и высокоскоростные, по размеру охваченной территории различают глобальные, региональные и локальные сети, по иерархической организации локальные сети бывают одноранговые и с выделенным сервером. Рассмотрим

основные характеристики и описание сетей согласно их делению по территориальной протяженности и иерархической организации.

Глобальные сети (Wide Area Networks, WAN) объединяют компьютеры, находящиеся на больших расстояниях друг от друга: в различных городах, в разных странах и на разных континентах. Глобальные сети могут объединять как отдельные компьютеры, так локальные и региональные сети.

Первая, самая большая и популярная глобальная сеть – это Интернет. По оценке Международного союза электросвязи ITU[1] (International Telecommunication Union) в 2015 г. количество пользователей сети Интернет достигнет 3,2 млрд, а согласно данным компании Netcraft в июне 2015 г. в сети Интернет работали 863 105 652 сайта. Ученые, исследователи-энтузиасты и дизайнеры пытаются визуально представить структуру Интернета. Существуют разные варианты такого представления. В приложении приведены ссылки на некоторые сайты с изображениями и картами сети Интернет, а на рис. 1.2 показана карта Интернета на 22 ноября 2003 г., созданная группой исследователей The Opte Project. Каждая линия на карте нарисована между двумя узлами сети.

К ***локальным сетям*** (Local Area Networks, LAN) относят сети компьютеров, сосредоточенные на небольшой территории (обычно в радиусе не более 1-2 км). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации. Исторически первыми появились глобальные сети, а уже после них локальные.

Также по территориальному признаку выделяют ***региональные сети***, или ***сети мегаполисов*** (Metropolitan Area Networks, MAN), которые предназначены для обслуживания территории крупного города или региона.

[1] Международный союз электросвязи – специализированное учреждение Организации Объединенных Наций (с 1947 г.) в области информационно-коммуникационных технологий, регулирует распределение радиочастотного спектра и спутниковых орбит в международном масштабе, разрабатывает технические стандарты и рекомендации в области телекоммуникаций и радио. Основан как Международный телеграфный союз в 1865 г.

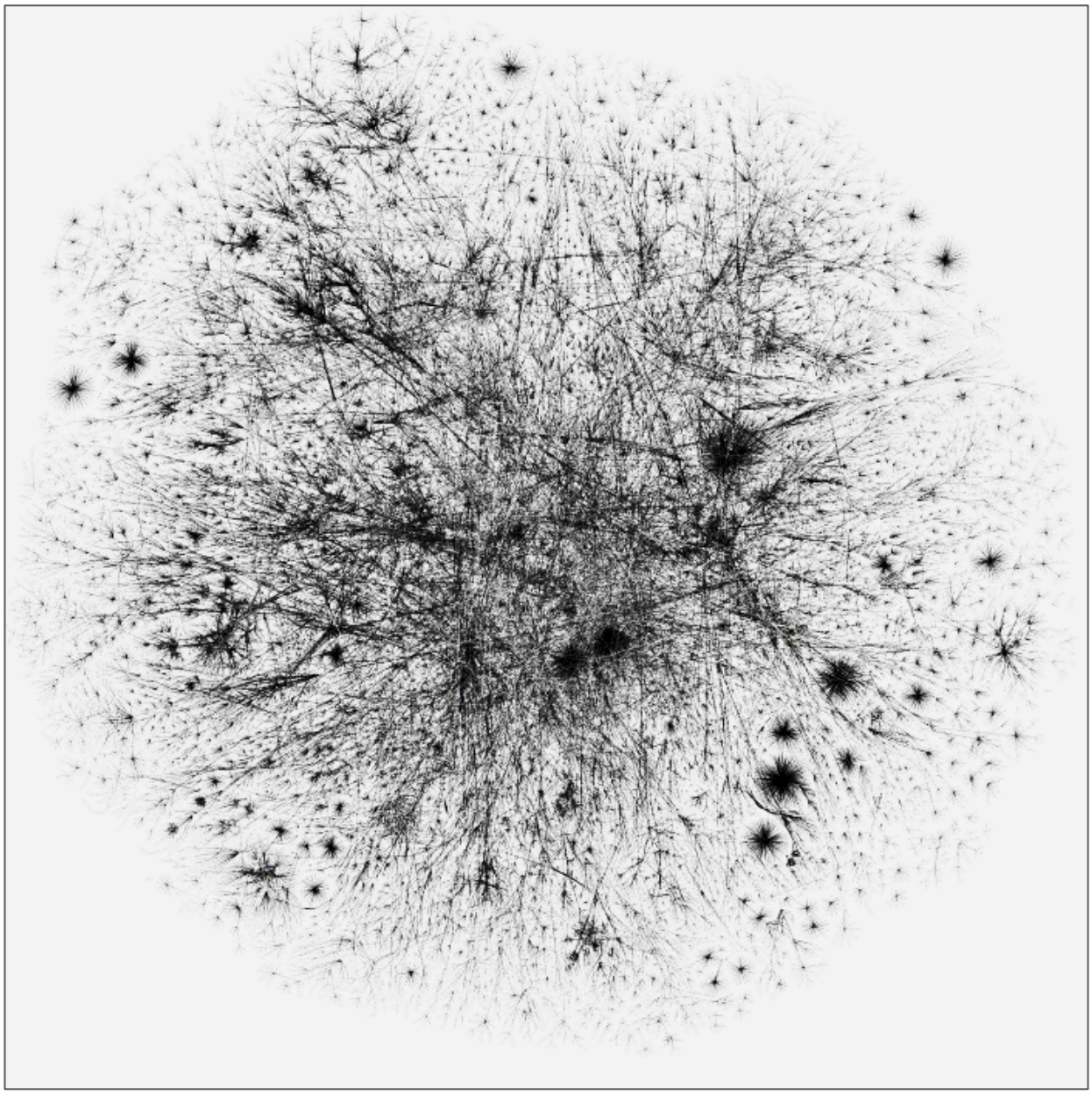


Рис. 1.2. Карта сети Интернет

Интересным случаем связи локальных и глобальных сетей является виртуальная частная сеть (англ. VPN, Virtual Private Network). Она создается предприятием путем объединения нескольких территориально разделенных локальных сетей своих филиалов с помощью глобальных сетей, например, Интернет (рис. 1.3). Для обеспечения безопасности такой сети применяются специальные технологии защищенного канала.

В зависимости от иерархической организации локальные сети бывают одноранговые и с выделенным сервером.

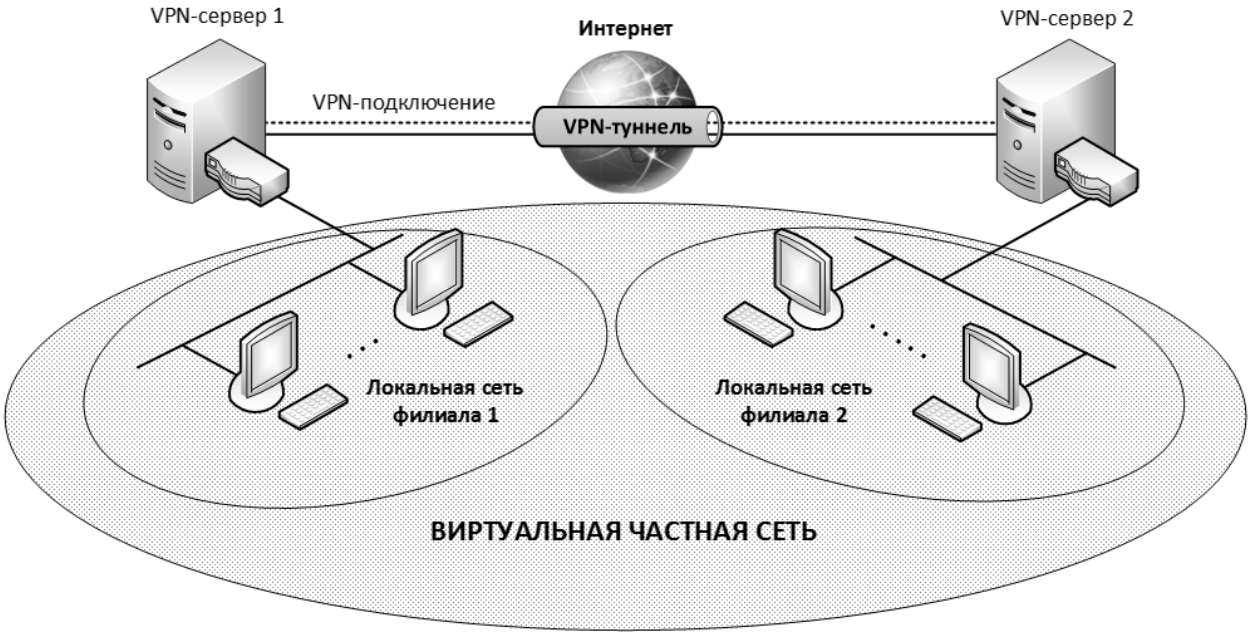


Рис. 1.3. Виртуальная частная сеть

Если в локальной сети нет отдельно выделенного сервера, а на всех компьютерах установлена операционная система, совмещающая функции клиента и сервера, то такая сеть называется ***одноранговой***. Компьютеры этой сети равноправны – ни один компьютер не может контролировать другой. Каждый компьютер может не только обращаться к ресурсам других компьютеров (файлам, принтерам и т. п.), но и предоставлять собственные ресурсы в распоряжение остальных пользователей сети (рис. 1.4). Однако из-за отсутствия управляющего компьютера каждый пользователь сам определяет права доступа к разделяемому ресурсу на своем компьютере. Кроме этого, в одноранговой сети доступ к общему ресурсу одновременно могут получить максимально от 10 до 20 участников сети.

Одноранговая сеть является наиболее простой и дешевой в создании. Поддержка таких сетей имеется в любой современной операционной системе, поэтому дополнительного программного обеспечения не требуется. Обычно в качестве одноранговых организуются сети небольших офисов и домашние сети.

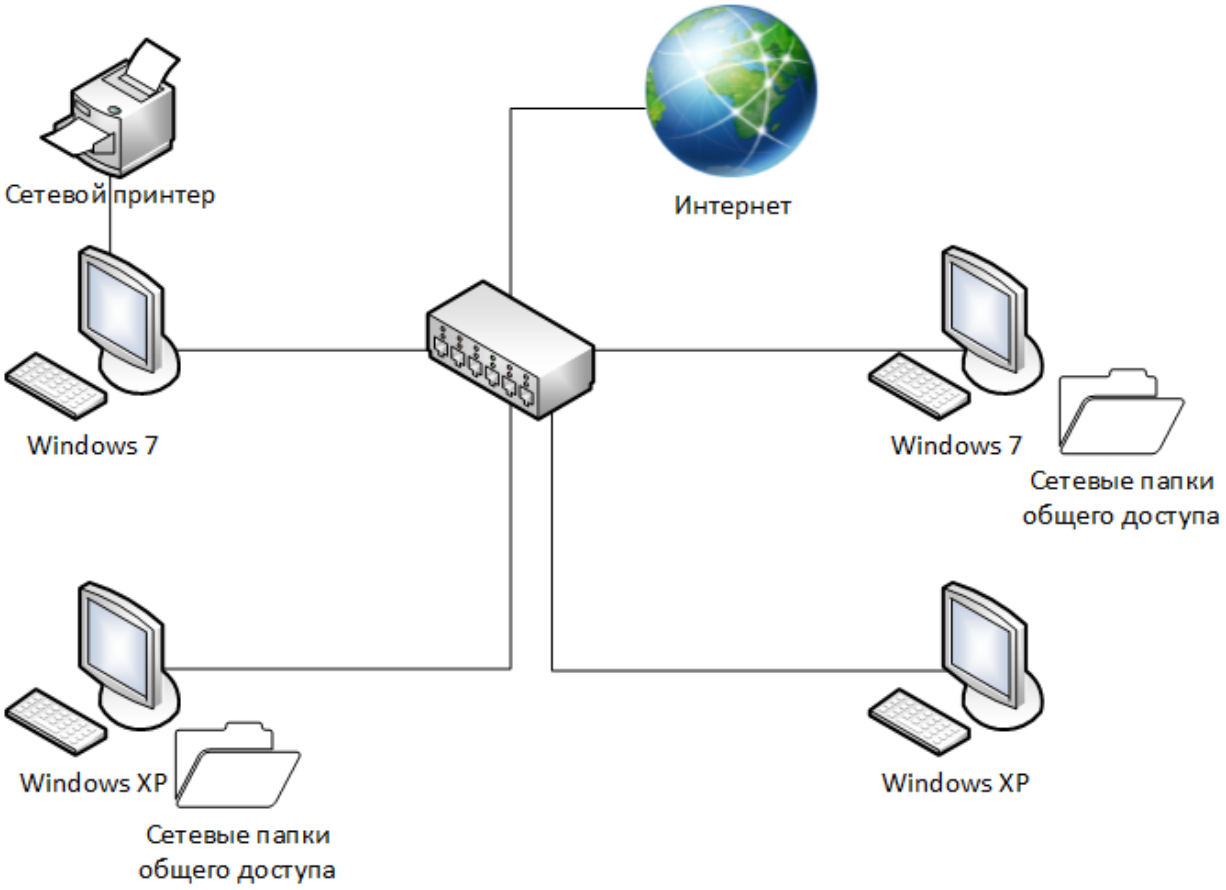


Рис. 1.4. Пример одноранговой сети

В ***сети с выделенным сервером*** один или более компьютеров с установленной на них серверной операционной системой и серверными программными модулями занимаются исключительно обслуживанием запросов других компьютеров.

Как правило, выделенный сервер характеризуется большой мощностью и быстродействием, достаточными для предоставления необходимых услуг остальным компьютерам сети. Это могут быть услуги по хранению и доступу к файлам (такой компьютер называется *файл-сервером*), по управлению очередью печати и доступу к общему принтеру (*принт-сервер* или *сервер печати*, рис. 1.5), по организации и управлению корпоративной электронной почтой (*почтовый сервер*), по доступу к единой базе данных автоматизированной информационной системы предприятия (*сервер базы данных*), например, системы бухгалтерского учета, и другие.

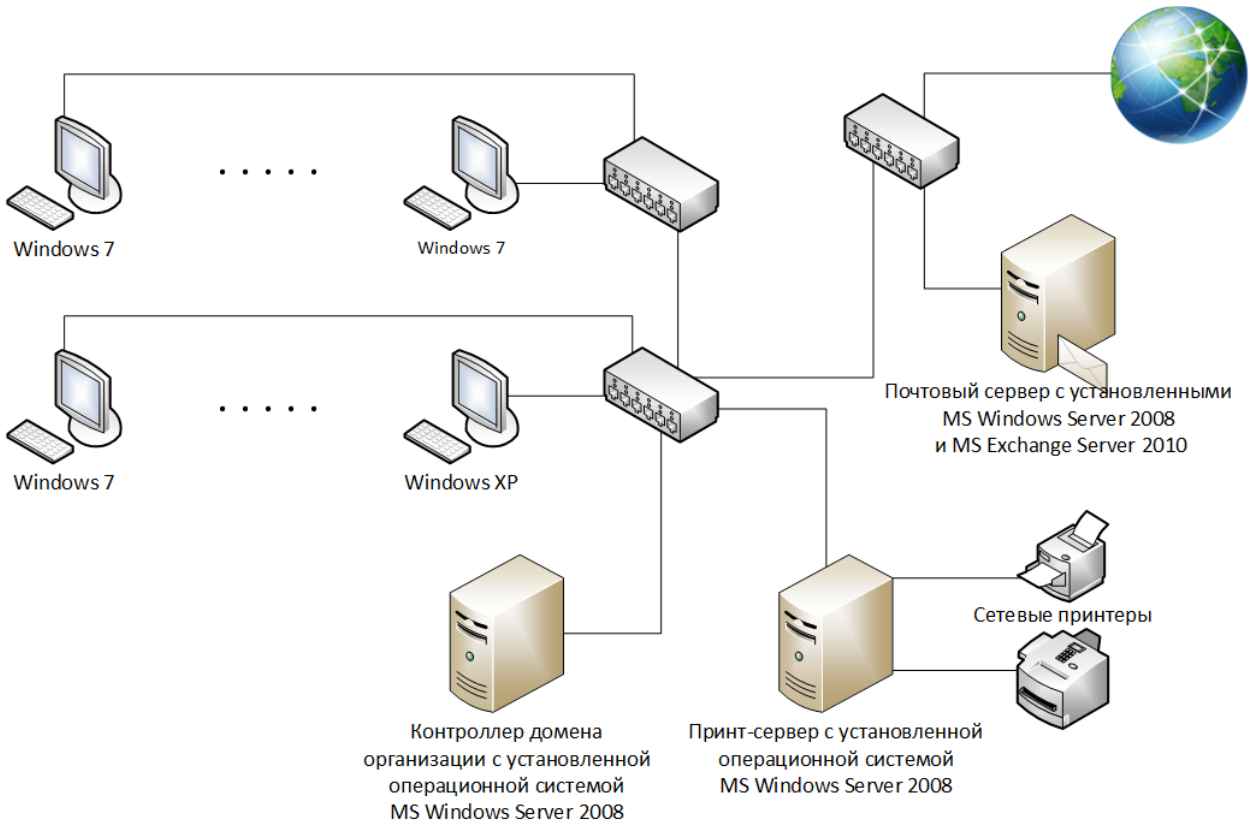


Рис. 1.5. Пример сети с тремя выделенными серверами

В большинстве случаев для упрощения администрирования и повышения уровня безопасности в локальной сети организации выделяется компьютер, называемый *контроллером домена*[1], отвечающий за управление учетными записями пользователей, контроля безопасности и настройки разрешений для всех компьютеров домена. Домен имеет уникальное имя и управляется как единый объект с применением общих правил и действий. Это позволяет легко менять настройки, так как изменения автоматически производятся для всех компьютеров. Для входа в систему компьютера, принадлежащего домену, пользователь должен указать данные своей учетной записи: имя пользователя и пароль (рис. 1.6).

Установленные на выделенных компьютерах серверные операционные системы отличаются от обычных, они обладают особыми характеристиками

[1] В данном случае домен – это совокупность компьютеров в сети, для которых существует общая база учетных записей пользователей и определена общая политика безопасности.

(например, поддержка нескольких процессоров, б*о*льшего объема оперативной памяти) и предоставляют больше инструментов для администрирования сети. Примерами таких операционных систем являются системы семейства Windows Server компании Microsoft, OS X Server компании Apple, Ubuntu Server и др.

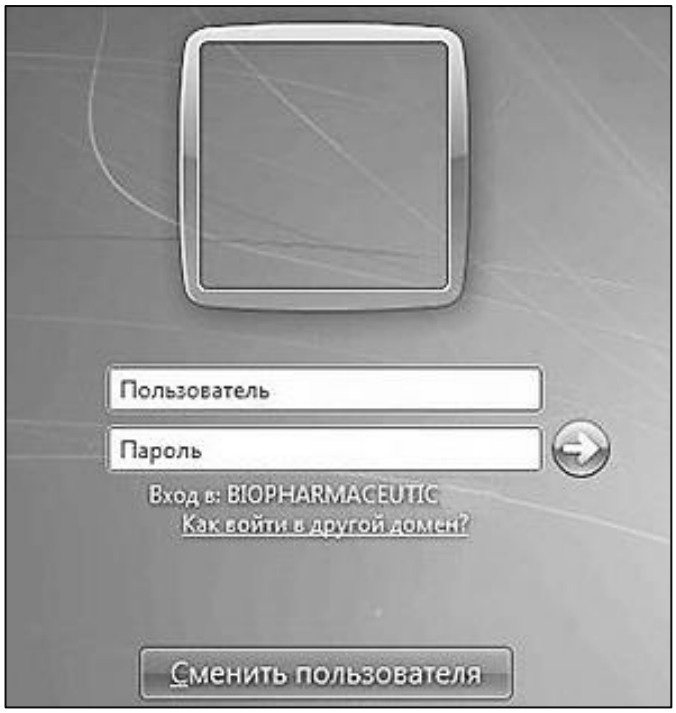


Рис. 1.6. Экран входа в домен BIOPHARMACEUTIC операционной системы Windows 7

1.3. Сетевые характеристики

Существует большое количество характеристик, связанных с передачей данных по сети. Рассмотрим некоторые из них, необходимые для понимания всеми пользователями.

Трафик (англ. traffic – движение, сообщение) – объем передаваемых по сети данных. Различают входящий трафик данных, получаемых компьютером из сети, и исходящий трафик данных, отправляемых компьютером в сеть.

Трафик измеряется в байтах, используются двоичные приставки кило (2^{10}), мега (2^{20}), гига (2^{30}), тера (2^{40}):

1 Кб = 1024 байта,

1 Мб = 1024 Кб,

1 Гб = 1024 Мб,

1 Тб = 1024 Гб.

Скорость передачи данных – это фактическая скорость потока данных, прошедшего через сеть. Определяется как отношение объема переданных данных за промежуток времени на продолжительность этого промежутка. Базовой единицей измерения скорости передачи данных является бит в секунду (бит/с, б/с, bps от англ. bits per second). Для образования из нее производных единиц измерения используются приставки международной системы единиц СИ кило (10^3), мега (10^6), гига (10^9), тера (10^{12}):

1 кбит/с (kbps, kbit/s) = 1000 бит/с,

1 Мбит/с (Mbps, Mbit/s) = 1000 кбит/с,

1 Гбит/с (Gbps, Gbit/s) = 1000 Мбит/с,

1 Тбит/с[1] (Tbps, Tbit/s) = 1000 Гбит/с.

Также используется более крупная единица – байт в секунду и ее производные:

1 Б/с (Bps от англ. Bytes per second) = 8 бит/с,

1 кБ/с (kB/s) = 1000 Б/с,

1 МБ/с (MB/s) = 1000 КБ/с.

Важно различать и не путать сокращения наименований: строчная буква «б» или английская «b» обозначают бит, а прописная «Б» или «В» – байт.

Пропускная способность – это максимально возможная скорость передачи данных по каналу связи. Пропускная способность зависит от качеств и характеристик физической среды передачи данных и используемой технологии передачи данных.

[1] В марте 2009 г. учёные из Датского технического университета первыми в мире преодолели «терабитный барьер» (1 Tbps) в скорости передачи данных по оптоволокну.

1.4. Прямое соединение двух компьютеров

Для того чтобы понять какие принципы лежат в основе построения и функционирования компьютерных сетей, рассмотрим простейший случай соединения двух компьютеров с целью общего доступа к файлам, называемое ***прямым соединением*** (рис. 1.7).

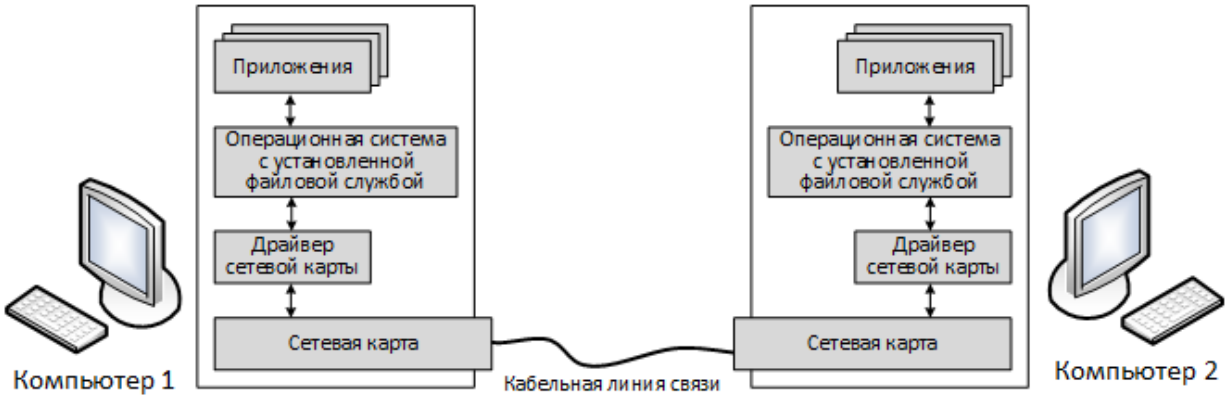


Рис. 1.7. Прямое соединение двух компьютеров

Во-первых, автономно работающие компьютеры необходимо физически соединить друг с другом, т. е. создать между ними линию связи, по которой будут передаваться данные и команды в форме электрических сигналов. Для этого на каждый компьютер устанавливается специальный аппаратный модуль, называемый сетевым адаптером или сетевой картой (в пользовательских компьютерах они, как правило, встроены в материнские платы). Сетевые карты связываются между собой кабелем, который подсоединяется к ним через соответствующие разъемы[1].

Чтобы операционная система и другие программы могли управлять сетевой картой и пользоваться её функциями, на каждом компьютере устанавливается специальная служебная программа – драйвер сетевой карты. Кроме этого, как говорилось выше, для доступа приложений и пользователей к

[1] Аналогичное соединение компьютеров возможно и с использованием беспроводных сетевых адаптеров по технологии Wi-Fi или Bluetooth.

разделяемым ресурсам на компьютерах должны быть установлены клиентский и серверный программные модули. В нашем случае, когда разделяемыми ресурсами являются файлы, эти модули образуют сетевую файловую службу, которая в самом простом варианте может быть встроена в операционную систему.

Как видим (рис. 1.7), в каждом отдельно взятом компьютере взаимодействие между приложениями, операционной системой, файловой службой, драйвером сетевой карты, самим устройством и линией передачи данных осуществляется на разных уровнях. На каждом из уровней соответствующее устройство или программа выполняет свой набор функций: физическую передачу данных по линии связи, обработку электрических сигналов в информационные, обработку возникающих ошибок, объединение отдельных информационных сигналов в целые сообщения, передачу этих сообщений определенному приложению и т. п. Важно, чтобы весь обмен сообщениями между разными уровнями одного компьютера или одинаковыми уровнями разных компьютеров осуществлялся по определенным правилам. Наборы таких правил представляют собой протоколы обмена данными в компьютерных сетях.

Таким образом, для создания компьютерной сети в общем случае необходимо: наличие линии связи между компьютерами, специальное аппаратное обеспечение – сетевое оборудование, специальные программные средства – сетевое программное обеспечение, и протоколы взаимодействия компонентов в сети.

Соединение двух автономных компьютеров является примером простейшей компьютерной сети. В действительности даже небольшая локальная сеть организации объединяет множество вычислительных устройств, а при создании протяженных сетей используется дополнительное сетевое оборудование и развитые технологии передачи данных.

1.5. Линии связи

Линия связи (или ***канал связи***) – это путь между двумя конечными узлами сети, который состоит из физической среды для передачи электрических информационных сигналов, аппаратуры передачи данных (например, модем) и промежуточной аппаратуры (например, усилители, мультиплексоры, коммутаторы). Физические среды можно разделить на два типа: проводные и беспроводные.

Проводные среды передачи данных

Проводные среды передачи предполагают наличие твердотельного проводника. К ним относятся медная витая пара, коаксиальный кабель, оптоволоконный кабель.

Витая пара (англ. twisted pair) представляет собой кабель, состоящий из одной или нескольких пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины) и покрытых внешней пластиковой оболочкой (рис. 1.8). Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

Витая пара существует в экранированном варианте STP (Shielded Twisted Pair, рис. 1.8), когда пара медных проводов обертывается в изоляционный экран, и неэкранированном UTP (Unshielded Twisted Pair, рис. 1.9), когда изоляционная обертка отсутствует.

Рис. 1.8. Экранированная витая пара

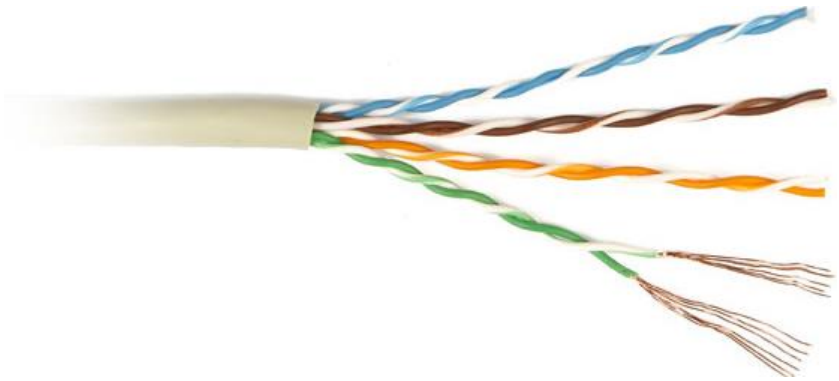


Рис. 1.9. Неэкранированная витая пара

Коаксиальный кабель (англ. coaxial cabel, рис. 1.10) состоит

– из внутреннего проводника *1* (медная жила);

– диэлектрической изоляции *2* (например, полиуретан);

– внешнего проводника *3*, который может быть полой медной трубкой или оплеткой;

– оболочки *4*, которая служит для изоляции и защиты от внешних воздействий.

Термин «коаксиальный» означает «соосный», «обладающий одной осью». Действительно, внешний проводник оплетается вокруг внутреннего проводника как вокруг оси.

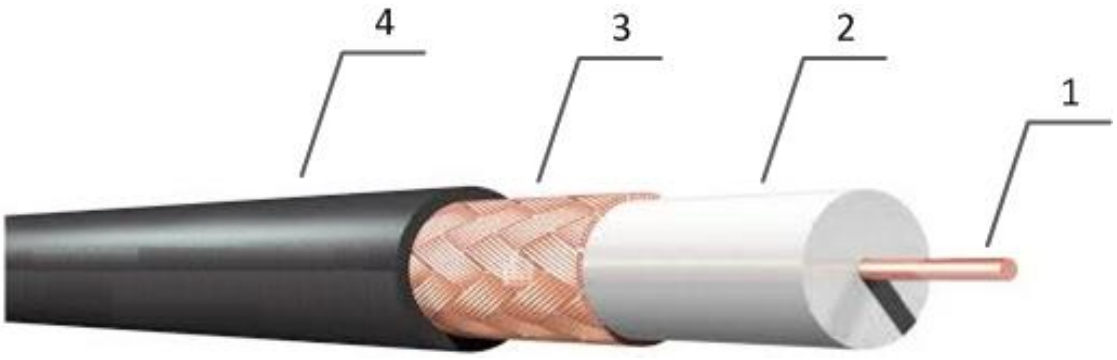


Рис. 1.10. Коаксиальный кабель

Внешний проводник играет двоякую роль – по нему передаются информационные сигналы и он является экраном, защищающим внутренний проводник от внешних электромагнитных полей.

В 1956 г. была проложена первая трансатлантическая телефонная линия ТАТ-1 (англ. Transatlantic No. 1) на базе коаксиального кабеля. Сегодня в сетевых технологиях коаксиал вытеснен витой парой и оптоволокном.

Волоконно-оптический кабель (англ. optical fiber) состоит из тонких (5 – 60 микронов, микрометров) гибких стеклянных волокон (волоконных световодов), по которым распространяются световые сигналы (рис. 1.11).

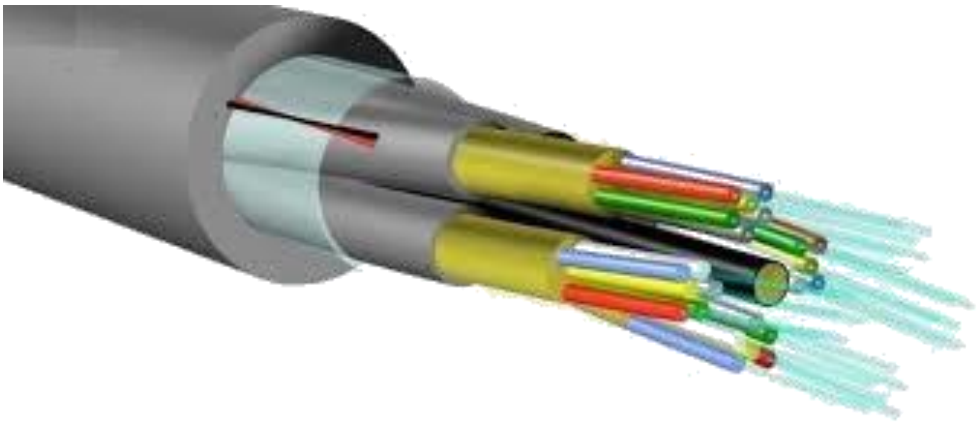


Рис. 1.11. Волоконно-оптический кабель

Это наиболее качественный тип кабеля – он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех. Каждый световод состоит из центрального проводника света (сердцевины), представляющего собой стеклянное волокно, и стеклянной оболочки, обладающей меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки. В качестве источника света применяются светодиодные излучатели или лазерные диоды.

Волоконно-оптический кабель применяется в качестве среды передачи в телекоммуникационных сетях различных уровней: от подводных межконтинентальных магистралей (см. ссылку на карту подводного кабеля в приложении) до домашних компьютерных сетей.

Беспроводная среда передачи данных

В ***беспроводной среде*** передача информации осуществляется на основе распространения электромагнитных волн через земную атмосферу или космическое пространство без участия твердых проводников.

Для построения беспроводной линии связи каждый узел оснащается антенной, которая одновременно является передатчиком и приемником электромагнитных волн. Антенны бывают двух типов – ***направленные***, когда электромагнитные волны распространяются от нее в определенном направлении в пределах одного сектора, и ***ненаправленные***, когда волны распространяются во всех направлениях и заполняют все пространство вокруг в пределах радиуса, определяемого затуханием мощности сигнала. На рис. 1.12 изображены параболическая антенна, которая является направленной, и ненаправленная антенна, представляющая собой вертикальный проводник.

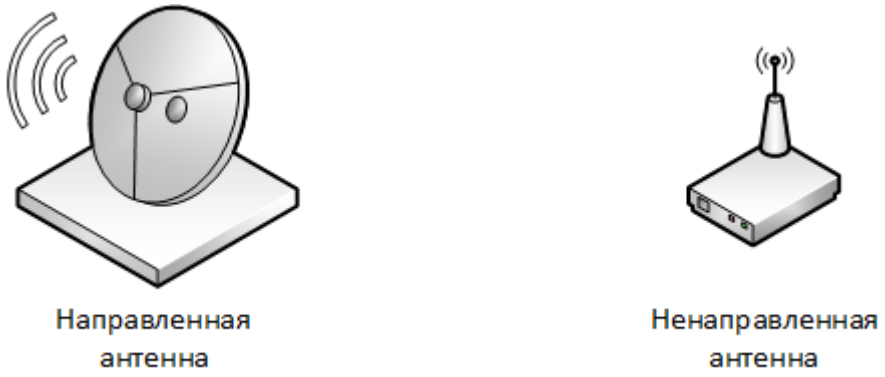


Рис. 1.12. Типы антенн

Электромагнитные волны распространяются в атмосфере или вакууме со скоростью 3*108 м/с. Диапазоны спектра электромагнитных волн частотой до 300 ГГц имеют общее стандартное название – радиодиапазон. В табл. 1.1 приведены диапазоны радиоволн с наименованием, обозначением, указанием частоты и длины волны, описанием области применения.

Таблица 1.1

Диапазоны радиочастот

Диапазоны радиочастот	**Сверхдлинные волны**		**Длинные волны**	**Средние волны**	**Короткие волны**	**Ультракороткие волны**			
							Микроволновые диапазоны		
Обозначение	ULF, SLF, ELF	VLF	LF	MF	HF	VHF	UHF	SHF	EHF
Длина волны	100000-100 км	100-10 км	10-1 км	1 км-100 м	100-10 м	10-1 м	1 м-10 см	10-1 см	10-1 мм
Частота	3-3000 Гц	3-30 кГц	30-300 кГц	300-3000 кГц	3 – 30 МГц	30 – 300 МГц	300 – 3000 МГц	3 – 30 ГГц	30 – 300 ГГц
Область применения	Подводная связь, геофизические исследования	Связь с подводными лодками, грозопеленгация, надводная связь	АМ-радио, радиосвязь			Телевизионный сигнал, FM-радио	Телевизионный сигнал, сотовые телефоны, Bluetooth, Wi-Fi (2.4 ГГц)	Спутники, радары, Wi-Fi (5 ГГц)	Спутники, радары

Чем выше частота, тем выше возможная скорость передачи информации, но тем хуже проникает сигнал через препятствия. Так низкочастотные радиоволны АМ-диапазонов легко проникают в дома, позволяя обходиться комнатной антенной, а для приема более высокочастотного сигнала телевидения часто требуется внешняя антенна. Сегодня потребность в скоростной передаче информации является преобладающей, поэтому все современные системы беспроводной передачи информации работают в высокочастотных (микроволновых) диапазонах, начиная с 800 МГц. Однако эти диапазоны отличаются высоким уровнем помех, которые создают внешние источники излучения, а также многократно отраженные от стен и других преград полезные сигналы. Поэтому в беспроводных системах связи применяют различные средства, направленные на снижение влияния помех. К таким средствам относятся, например, специальные коды коррекции ошибок и протоколы с подтверждением доставки информации.

Для решения проблемы разделения электромагнитного спектра различными операторами связи и организациями для осуществления беспроводной передачи информации в каждой стране есть специальный государственный орган, который выдает этим организациям ***лицензии на использование определенной части спектра***. Лицензия выдается на определенную территорию, в пределах которой оператор использует закрепленный за ним диапазон частот монопольно.

Также существуют частотные диапазоны 900 МГц, 2.4 ГГц, 5 ГГц, которые рекомендованы ITU как диапазоны для международного использования без лицензирования. Эти диапазоны используются для беспроводной связи в промышленных товарах общего назначения, например, в устройствах блокирования дверей автомобилей, научных и медицинских приборах, а также в технологиях Bluetooth и Wi-Fi (сокращение от англ. Wireless Fidelity – беспроводная точность).

Аппаратура линий связи

Как было сказано выше, кроме физической среды передачи данных в состав линии связи входит также аппаратура приема-передачи данных и промежуточная аппаратура.

Аппаратура приема-передачи данных в компьютерных сетях непосредственно присоединяет компьютеры к линиям связи и отвечает за передачу информации в физическую среду и прием из нее сигналов нужной формы, мощности и частоты. Примерами аппаратуры передачи данных могут служить сетевой адаптер и модем.

Сетевой адаптер (сетевая карта, сетевая интерфейсная карта, NIC – Network Interface Card) – аппаратный модуль, подключаемый к вычислительному устройству и предназначенный для соединения этого устройства с сетью. Для подсоединения к сети по технологии Wi-Fi используются беспроводные адаптеры (рис. 1.13).

Рис. 1.13. Беспроводной сетевой адаптер

Сетевые карты бывают в виде плат расширения, которые устанавливаются в соответствующий слот материнской платы (рис. 1.13, 1.14), в виде от-

дельных устройств, подключаемых через порт USB, или могут быть встроенными в материнские платы.

Рис. 1.14. Сетевой адаптер в виде платы расширения

Модем (МОдулятор-ДЕМодулятор) – устройство, выполняющее преобразование цифровых сигналов (потоков бит) в аналоговую форму, для передачи их по каналам связи аналогового типа (например, телефонным линиям связи), а также преобразование принимаемых аналоговых сигналов в цифровую форму для обработки их вычислительным устройством (рис. 1.15).

Рис. 1.15. Внешний вид модема Acorp

Промежуточная аппаратура используется на линиях связи большой протяженности и предназначена для улучшения качества сигнала и создания

постоянного канала связи между двумя абонентами сети. К промежуточной аппаратуре относятся ***усилители***, повышающие мощность сигнала, ***регенераторы***, повышающие мощность и восстанавливающие форму импульсных сигналов, ***мультиплексоры***, образующие из нескольких отдельных потоков данных общий поток, который передается по одному физическому каналу данных, ***демультиплексоры***, разделяющие суммарный поток на несколько составляющих его потоков данных, и др.

1.6. Топология компьютерных сетей

В рассмотренном случае прямого соединения двух компьютеров возможен только один вариант их связи. При объединении в сеть нескольких узлов, уже возникают разные варианты связи этих узлов между собой (рис. 1.16). Таким образом, при построении компьютерной сети, состоящей из множества устройств, появляется задача выбора ее топологии.

Топология сети – схема расположения и соединения сетевых устройств.

От выбора топологии связей существенно зависят характеристики сети. Например, наличие между узлами нескольких путей повышает надежность сети и делает возможным распределение загрузки между отдельными каналами.

Различают следующие топологии компьютерных сетей:

- полносвязную;
- ячеистую;
- кольцевую;
- звездообразную («звезда»);
- древовидную;
- общую шину;
- смешанную.

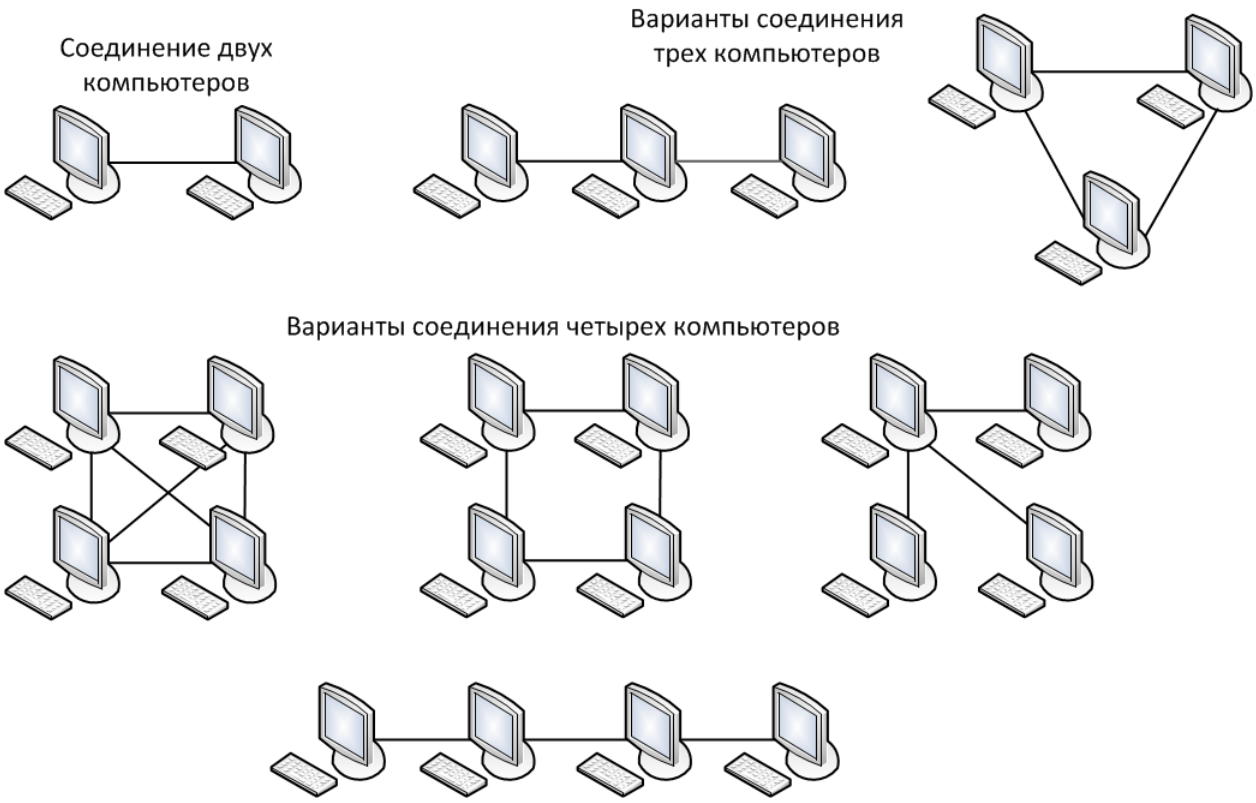


Рис. 1.16. Способы соединения компьютеров

Полносвязная топология соответствует сети, в которой каждый компьютер непосредственно связан со всеми остальными (рис. 1.17).

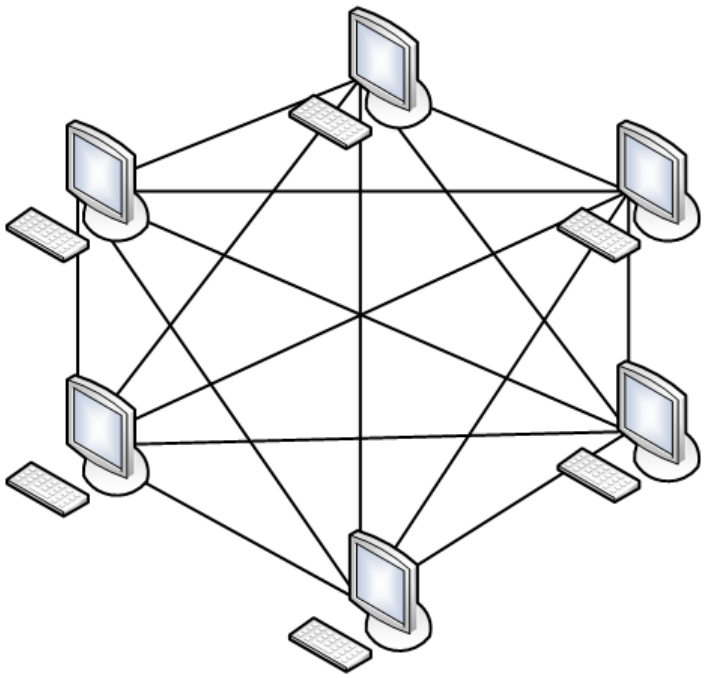


Рис. 1.17. Полносвязная топология

Из-за большого количества связей между узлами данный вариант является самым надежным, но в тоже время громоздким и неэффективным: каждый компьютер должен иметь достаточное количество коммуникационных портов (следовательно, сетевых адаптеров) для связи с каждым из остальных компьютеров сети. Кроме этого для каждой пары компьютеров должна быть выделена отдельная физическая линия связи. Поэтому в крупных сетях полносвязная топология применяются редко.

Ячеистая топология образуется из полносвязной путем удаления некоторых линий связей (рис. 1.18). Такая топология допускает соединение большого числа компьютеров и характерна, как правило, для крупных сетей. Из рис. 1.10 видно, что в сетях могут использоваться как индивидуальные линии (каналы) связи между компьютерами, так и разделяемые, когда одна линия связи попеременно используется несколькими компьютерами.

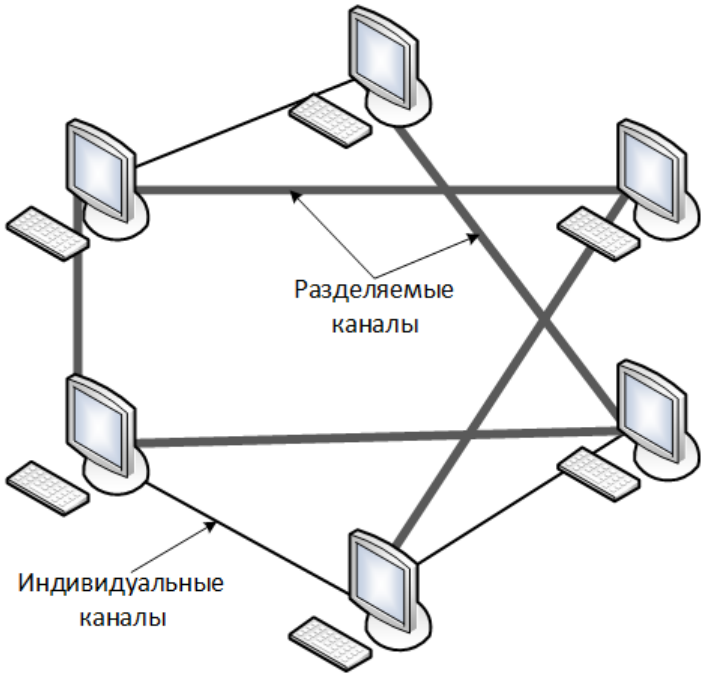


Рис. 1.18. Ячеистая топология

В ***кольцевой топологии*** (рис. 1.19) компьютеры объединяются между собой круговой связью, а данные передаются по кольцу от одного компьютера к другому. На каждом из компьютеров должно быть два коммуникаци-

онных порта: для связи с предыдущим компьютером и со следующим. Любая пара компьютеров соединена двумя путями – по часовой стрелке и против. Это обеспечивает резервную связь между узлами. Однако в сетях с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения одного компьютера не прерывался канал связи между остальными.

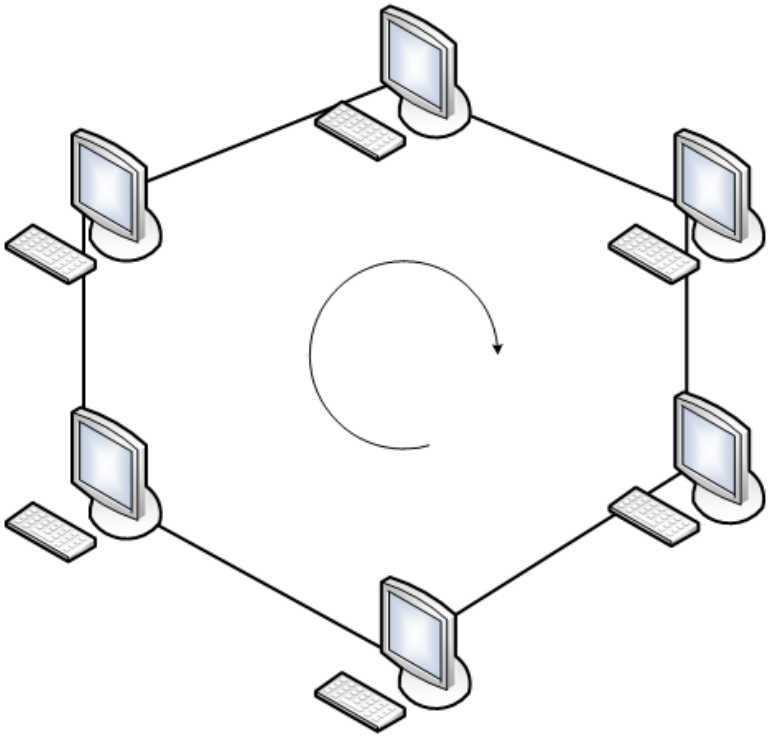


Рис. 1.19. Кольцевая топология

В ***звездообразной топологии*** каждый компьютер подключается при помощи отдельного кабеля к общему центральному устройству, в функции которого входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети (рис. 1.20).

В качестве такого центрального устройства чаще всего используется специальное сетевое оборудование: концентратор, коммутатор или маршрутизатор, однако может использоваться и универсальный компьютер с установленным специальным программным обеспечением и достаточным количеством коммуникационных портов.

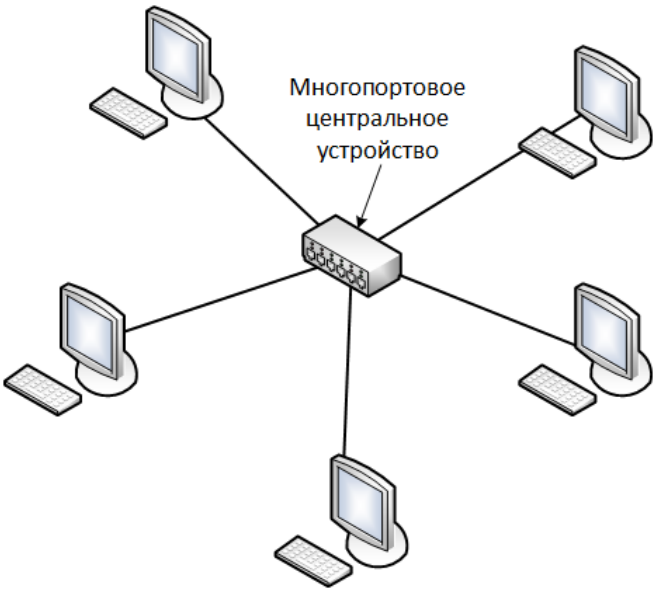


Рис. 1.20. Звездообразная топология

Если сеть строится с помощью иерархического соединения центральных устройств нескольких сетей звездообразной топологии, то образуется топология ***дерево*** или ***иерархическая звезда*** (рис. 1.21). В настоящее время данная топология является самой распространенной как в локальных, так и в глобальных сетях.

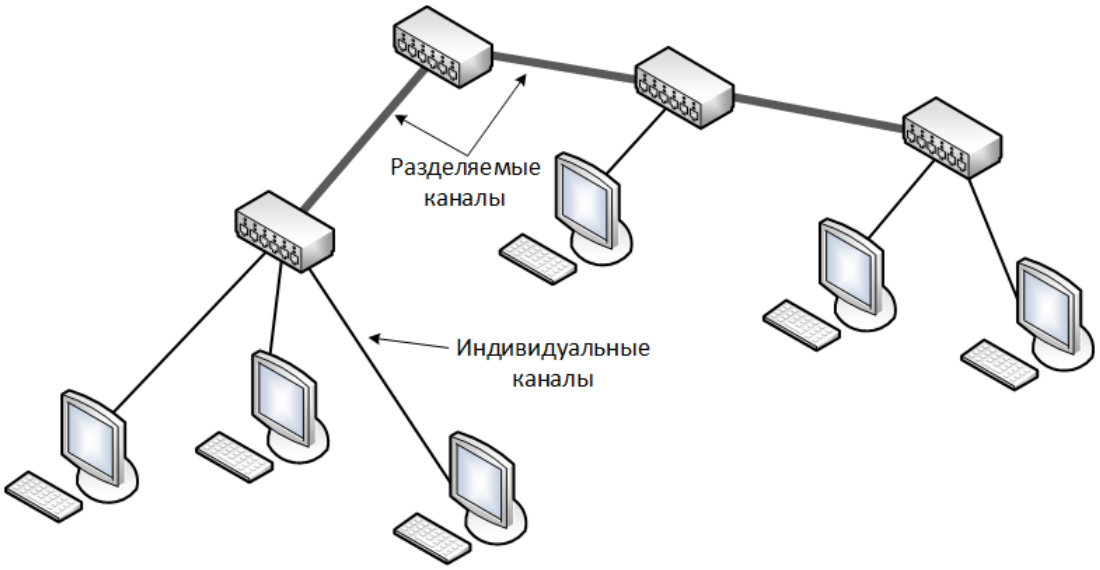


Рис. 1.21. Древовидная топология

В топологии ***общая шина*** все компьютеры подключаются к общему центральному элементу, в качестве которого выступает кабель или радиосреда

(рис. 1.22). Передаваемая информация распространяется по общей шине и доступна одновременно всем присоединенным к ней компьютерам, поэтому задача каждого компьютера – проверить кому адресовано сообщение. Недостатком такой топологии является зависимость скорости передачи данных от количества подключенных узлов: чем больше компьютеров и других узлов, тем ниже скорость передачи данных. Кроме этого, в случае повреждения центрального кабеля полностью парализуется вся сеть.

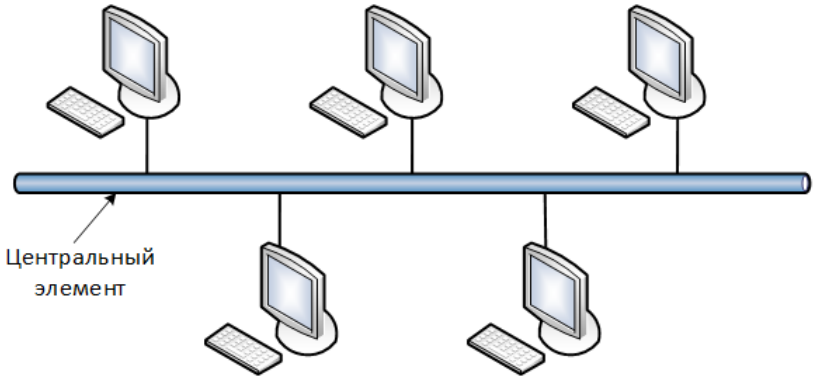


Рис. 1.22. Топология общая шина

Небольшие сети, как правило, строятся по типовой топологии (звезда, кольцо или общая шина). Крупные сети обычно имеют ***смешанную топологию***, которая объединяет отдельные подсети, имеющие разные типовые топологии (рис. 1.23).

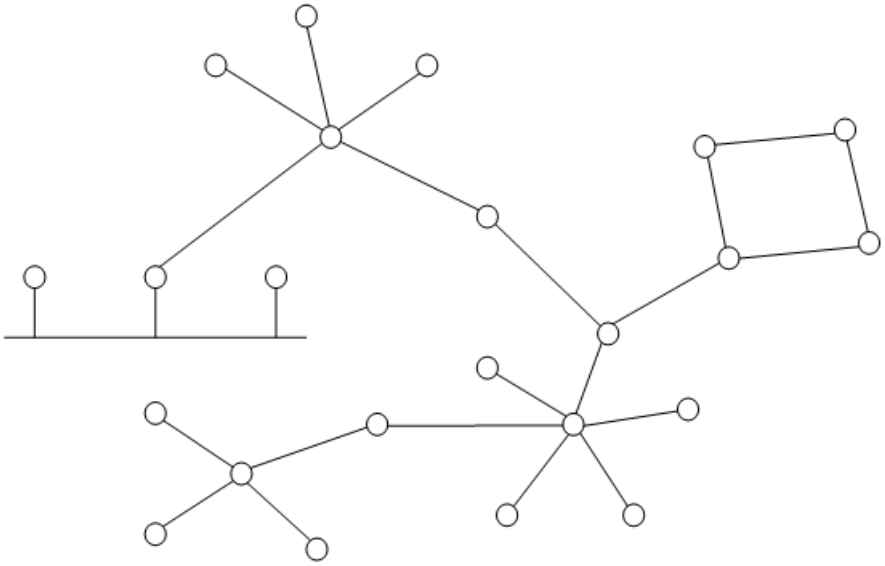


Рис. 1.23. Смешанная топология

1.7. Оборудование для связи компьютеров

Для объединения компьютеров в сеть согласно топологии «звезда» и «дерево» или объединения нескольких сетей в смешанную топологию используются специальные устройства связи: концентраторы, мосты, коммутаторы, маршрутизаторы. Рассмотрим их подробнее.

Концентратор (хаб, англ. hub) – простейшее устройство для соединения компьютеров в сеть. Его главной задачей является принять, усилить и распространить поступивший по одному из портов сигнал на все остальные порты. Никакой другой обработке сигнал в концентраторе не подвергается и абсолютно не важно, какого типа данные и кому передаются – в любом случае данные транслируются сразу на все порты, что увеличивает трафик в сети, уменьшая полезную скорость. Кроме этого, концентраторы не обрабатывают столкновения (коллизии), которые возникают, когда два или более устройств, подключенных к концентратору, пытаются одновременно передавать данные в сеть. При коллизии устройства самостоятельно прекращают передачу и возобновляют попытку через случайный промежуток времени ожидания.

Внешне концентратор представляет собой устройство, содержащее обычно от 4 до 32 портов (гнезд) и светодиоды, отображающие их активность (рис. 1.24).

Рис. 1.24. Внешний вид концентратора COMPEX PS2216

К портам можно подключать не только компьютеры, но и другие концентраторы, формируя таким образом сложные топологии типа «дерево».

Концентраторы также применялись в качестве усилителя сигнала для увеличения протяженности сети. В сетях, использующих коаксиальный кабель, концентраторы принято было называть повторителями, или репитерами (англ. repeater).

Сетевой мост (англ. bridge) – это устройство, используемое для объединения в единую сеть разнородных сегментов сети, часто с разной топологией. Его можно также использовать в качестве повторителя для увеличения длины сегментов локальной сети и увеличения количества подключений. Мост является более «интеллектуальным» устройством, чем коммутатор: он умеет определять аппаратный адрес источника и приемника сигнала, а также применяя аппаратную реализацию разных алгоритмов, мост позволяет фильтровать и разделять траффик, устраняя проблему возникновения большого числа коллизий. Внешне мост имеет небольшой размер и содержит минимальное количество портов (рис. 1.25).

Рис. 1.25. Внешний вид беспроводного моста 3Com

Подавляющее большинство современных компьютерных сетей строится на коммутаторах и маршрутизаторах. Концентраторы были вытеснены сначала мостами, а затем коммутаторами, выполняющими аналогичные мосту функции.

Коммутатор (свитч, англ. switch) – основное устройство, применяемое в качестве центрального узла для подключения компьютеров в сетях топологии «звезда». Имеет бо́льшую функциональность, чем концентратор, в отличие от которого не транслирует данные на все имеющиеся порты, а отправляет их на конкретный порт, уменьшая тем самым время доставки. В отличие от моста коммутатор может выстраивать большое число виртуальных каналов связи между портами, т. е. коммутировать порты друг с другом (отсюда название устройства), производя параллельную обработку данных, поступающих с разных портов. Как правило, коммутатор содержит не более 48 портов (рис. 1.26). В крупных локальных сетях применяются стоечные коммутаторы, предназначенные для установки в монтажный шкаф.

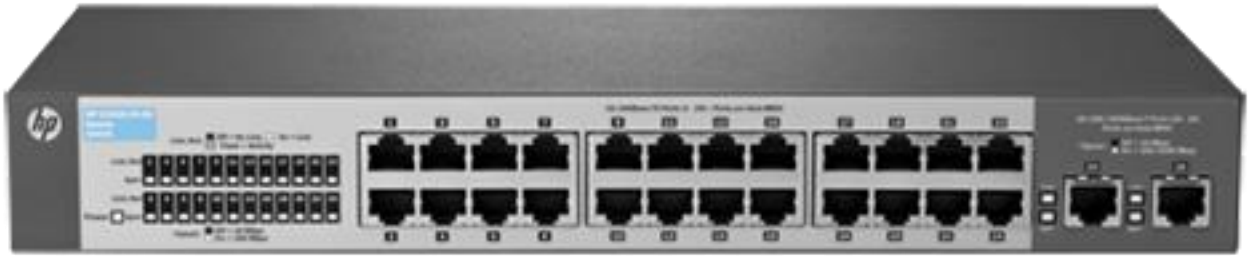


Рис. 1.26. Внешний вид коммутатора HP

Маршрутизатор (роутер, англ. router) – наиболее «интеллектуальное» из всех перечисленных устройств, в задачу которого входит анализ адресов, определение наилучшего маршрута доставки пакета данных по назначению (рис. 1.27). Маршрутизаторы могут выполнять все, что концентраторы, мосты и коммутаторы вместе взятые: как и концентраторы они восстанавливают уровень и форму передаваемого сигнала, как мосты и коммутаторы – позволяют избежать коллизий. Кроме этого, маршрутизаторы умеют выполнять целый ряд весьма сложных действий, например, обнаруживать проблемы в сети и сообщать о них, вести статистику полученных и переданных данных, фильтровать данные и т. д.

Рис. 1.27. Внешний вид маршрутизатора EdgeRouter

Мощные маршрутизаторы являются довольно сложными и дорогими программно-аппаратными устройствами, поэтому в современных сетях их иногда заменяют так называемыми ***коммутаторами 3-го уровня*** (по номеру уровня модели OSI) – устройствами, занимающими промежуточную ступень между коммутаторами и маршрутизаторами. От обычных коммутаторов они отличаются тем, что могут выполнять простейшие функции маршрутизации, оставаясь при этом производительными и не очень дорогими.

Под ***шлюзом*** (англ. gateway) подразумевается устройство, соединяющее разные сетевые архитектуры[1] (например, шлюз из технологии Ethernet в Token Ring). Шлюз должен иметь физические порты для подключения разнородных систем и «понимать» разнородные протоколы, выступая для них в роли «переводчика».

Типичным примером шлюзов являются широко используемые в современных домашних сетях интегрированные устройства, в которых объединены ADSL-модем для подключения к Интернету через телефонную линию, беспроводная точка доступа Wi-Fi и коммутатор, работающий по технологии Fast Ethernet.

[1] В общем случае под шлюзом обычно понимается любое устройство или программа, позволяющие объединять разнородные системы. Например, существуют Интернет-шлюзы являющиеся, как правило, программным обеспечением для организации передачи трафика между разными сетями, или почтовые шлюзы, используемые для связи разных систем электронной почты.

1.8. Сетевое программное обеспечение

К сетевому программному обеспечению относятся сетевые службы, сетевые операционные системы и сетевые приложения.

Сетевые службы включают в себя клиентскую и серверную части. Обе части, либо только одна из них, могут быть встроенными в операционную систему или существовать в виде отдельных программных продуктов. Например, сетевая файловая служба и служба печати обычно встраиваются в операционную систему, а веб-сервер и веб-браузер устанавливаются как отдельные приложения.

Сетевой операционной системой называют операционную систему, которая кроме управления локальными ресурсами компьютера предоставляет пользователям и приложениям возможность эффективного и удобного доступа к информационным и аппаратным ресурсам других компьютеров сети. Сегодня практически все операционные системы являются сетевыми. Особое место занимают специальные варианты сетевых операционных систем, предназначенные для работы в роли серверов и называемые серверными операционными системами.

Приложения, выполняемые на подключенном к сети компьютере, могут быть трех типов:

- локальными приложениями;
- централизованными сетевыми приложениями;
- распределенными сетевыми приложениями.

Локальное приложение целиком выполняется на данном компьютере и использует только локальные ресурсы. Для такого приложения не требуется никаких сетевых средств, оно может быть выполнено на автономно работающем компьютере. ***Централизованное сетевое приложение*** целиком выполняется на данном компьютере, но обращается в процессе своего выполнения к ресурсам других компьютеров в сети.

Распределенное сетевое приложение состоит из нескольких взаимодействующих частей, каждая из которых выполняет какую-то определенную законченную работу по решению прикладной задачи. Каждая часть распределенного приложения может выполняться и, как правило, выполняется на отдельном компьютере сети. Очевидным преимуществом распределенных приложений является возможность распараллеливания вычислений, а также специализация компьютеров. Все сетевые службы по определению относятся к классу распределенных приложений.

1.9. Стеки протоколов и модель OSI

Организация взаимодействия между устройствами сети является сложной задачей. Компьютерные сети объединяют самые разнообразные устройства с установленным на нем различным сетевым программным обеспечением. Кроме этого для реализации взаимодействия устройств сети необходимо реализовать множество функций: построение маршрута следования данных, кодирование и декодирование передаваемых данных, физическую передачу данных по линиям связи и т. д. Поэтому для организации взаимодействия компьютеров в сети применяется многоуровневый подход, в котором на каждом уровне от самого низкого – уровня передачи битов, и до самого высокого, реализующего обслуживание пользователей сети, действуют определенные соглашения и правила.

Протоколом называется совокупность правил, регламентирующих формат и процедуры обмена информацией между двумя или несколькими независимыми устройствами или программными приложениями. С помощью сетевых протоколов происходит обмен информацией между разными устройствами сети. Сетевые протоколы могут быть реализованы как программно, так и аппаратно. Например, для доступа к веб-сайтам в любой программе-браузере реализован протокол HTTP, а для подключения к сети и фи-

зической передачи и приему данных сетевой Ethernet-адаптер реализует протокол Ethernet.

Стеком протоколов называется иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети. Слово «стек» (от англ. stack – стопка) подразумевает, что каждый следующий уровень протоколов работает поверх предыдущего. Передаваемые сообщения последовательно проходят уровень за уровнем от верхнего к нижнему при отправке и от нижнего к верхнему при получении. Протоколы нижних уровней стека часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней – как правило, только программными средствами.

Примерами известных стеков протоколов являются: TCP/IP (стек Интернета), IPX/SPX (фирменный стек компании Novell), NetBIOS/SMB (стек компаний IBM и Microsoft) и др. С 1998 г. стек TCP/IP вышел в лидеры по числу установленных копий.

В начале 1980-х гг. несколько международных организаций, в число которых входили Международная организация по стандартизации ISO (International Organization for Standartization) и Международный союз электросвязи ITU, разработали ***сетевую модель OSI***[1], объясняющую как должна работать сеть. Модель OSI является теоретической и ее назначение состоит в обобщенном представлении средств сетевого взаимодействия. Модель OSI определяет уровни взаимодействия систем в сетях, стандартные названия этих уровней и функции, которые должен выполнять каждый уровень.

В модели OSI функции для организации взаимодействия устройств компьютерной сети делятся на семь уровней (табл. 1.2): прикладной, представ-

[1] Модель OSI (Open System Interconnection) – стандартная модель взаимодействия открытых систем. Здесь под открытой системой подразумевается сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами по стандартным правилам, определяющим формат, содержание и значение принимаемых и отправляемых сообщений.

ления, сеансовый, транспортный, сетевой, канальный и физический. Модель OSI не описывает конкретные наборы протоколов.

Таблица 1.2

Функциональное назначение уровней модели OSI

Номер	Название	Назначение
7	Прикладной уровень	Отвечает за взаимодействие с прикладными программами, с помощью которых пользователи сети получают доступ к разделяемым ресурсам
6	Уровень представления	Обеспечивает представление передаваемой по сети информации. За счет этого уровня информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. На этом уровне могут выполнять кодирование и перекодирование данных, шифрование и дешифрование данных
5	Сеансовый уровень	Управляет взаимодействием сторон: фиксирует какая из сторон является активной в настоящий момент, и предоставляет средства синхронизации сеанса. На этом уровне координируется связь между двумя рабочими узлами сети
4	Транспортный уровень	Обеспечивает приложениям или верхним уровням модели передачу данных с той степенью надежности, которая им требуется
3	Сетевой уровень	Служит для образования единой транспортной системы, объединяющей различные сети; отвечает за определение маршрута следования пересылаемых данных
2	Канальный уровень	Отвечает за установление соединения между взаимодействующими узлами, согласование в рамках соединения скоростей передатчика и приемника, обнаружение и коррекцию ошибок
1	Физический уровень	Отвечает за передачу потока битов по физическим каналам связи

Каждый из представленных уровней взаимодействует только с тем уровнем, который находится непосредственно под или над ним (рис. 1.28).

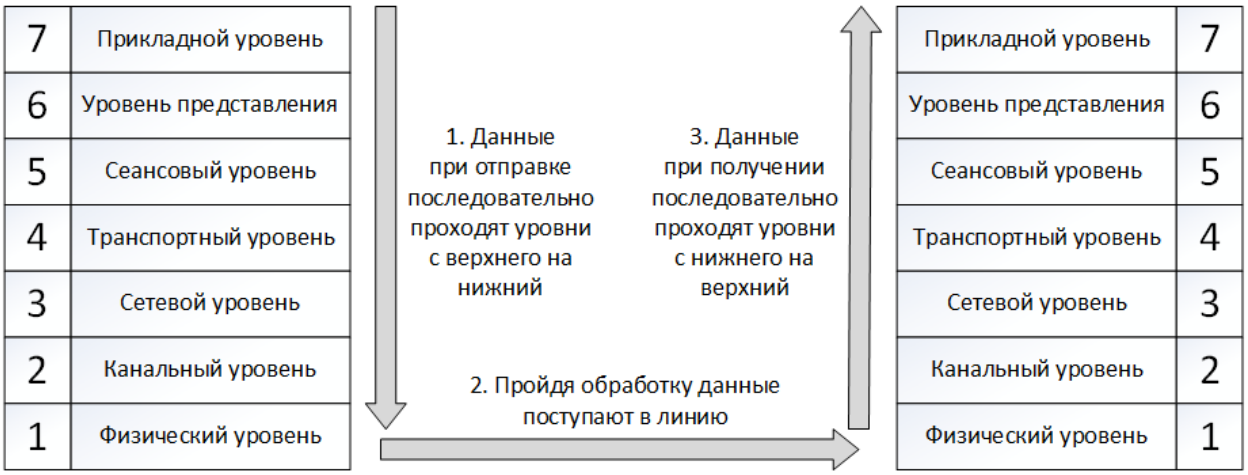


Рис. 1.28. Модель OSI описывает механизм перемещения данных в сети

Используемые на практике стеки протоколов часто не соответствуют разбиению на уровни модели OSI. Например, в стеке TCP/IP функции сеансового и представительного уровня объединены с прикладным уровнем. Такое несоответствие связано с тем, что модель OSI, по сути являющаяся справочной, появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

Рассмотрим подробнее стек протоколов TCP/IP, являющийся на сегодняшний день самой популярной технологией при построении компьютерных сетей и использующийся почти во всех существующих и вновь создаваемых локальных и глобальных сетях. Любая операционная система обязательно включает программную реализацию этого стека в своем комплекте поставки.

Название стека протоколов TCP/IP образовано из аббревиатур двух его основных протоколов: протокола управления передачей TCP (Transmission Control Protocol) и межсетевого протокола IP (Internet Protocol). Стек протоколов TCP/IP имеет 4 уровня (табл. 1.3): прикладной, транспортный, сетевой,

уровень сетевых интерфейсов. Прикладной уровень соответствует трем верхним уровням модели OSI: прикладному, представления и сеансовому. Он объединяет службы, предоставляемые системой пользовательским приложениям.

Таблица 1.3

Иерархическая структура стека TCP/IP

Уровни	Используемые протоколы
Прикладной уровень	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SNMP, SNTP и др.
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, RIP и др.
Уровень сетевых интерфейсов	Не регламентируется

За все время применения в компьютерных сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов прикладного уровня. К ним относятся такие распространённые протоколы,

– как протокол передачи гипертекста HTTP (HyperText Transfer Protocol) и его расширение HTTPS (HyperText Transfer Protocol Secure), поддерживающее шифрование;

– протокол передачи файлов FTP (File Transfer Protocol);

– простой протокол передачи электронной почты SMTP (Simple Mail Transfer Protocol);

– протоколы для извлечения электронной почты с сервера POP3 (Post Office Protocol Version 3 – почтовый протокол версии 3) и IMAP (Internet Message Access Protocol – протокол доступа к сообщениям в сети Интернет);

– протокол синхронизации времени по компьютерной сети SNTP (Simple Network Time Protocol), а также другие.

1.10. Аппаратный MAC-адрес

Аппаратный MAC-адрес (англ. Media Access Control – управление доступом к передающей среде) – это уникальный номер, присваиваемый сетево-

му оборудованию производителем при его изготовлении. MAC-адрес позволяет уникально идентифицировать каждый узел сети, и применяется администраторами сетей при конфигурировании и настройке локальных сетей организаций.

Как правило, MAC-адрес состоит из 6 байт (48 бит) и три старшие байта являются уникальным идентификатором организации-производителя. Адресное пространство насчитывает 2^{48} = 281 474 976 710 656 адресов. На рис. 1.29 показана маркировка сетевой карты с указанием ее MAC-адреса.

Рис. 1.29. MAC-адрес сетевой карты

1.11. Цифровой IP-адрес

Цифровой IP-адрес версии 4 (IPv4) имеет длину 4 байта. Для удобства представления он записывается в виде четырех десятичных чисел, разделенных точками. Каждое число – это однобайтное значение (от 0 до 255):

192.45.9.200

В двоичном формате этот же IP-адрес выглядит следующим образом:

10000000 00101101 00001001 10001000

IP-адрес содержит полную информацию, необходимую для идентификации компьютера в сети. Он состоит из двух частей: старшей – номера сети и младшей – номера узла в этой сети. Такое деление позволяет передавать

данные между сетями только на основании номера сети, а номер узла используется после доставки данных в нужную сеть. Подобным образом название улицы используется почтальоном только после того, как письмо доставлено в нужный населенный пункт.

В записи IP-адреса не предусматривается специальный разграничительный знак между номером сети и номером узла. Распространенным подходом определения положения границы между номером сети и номером узла в адресе является использование классов адресов. Введено 5 классов IP-адресов: A, B, C, D и E. Три из них – A, B и C – служат для адресации сетей и узлов, а два – D и E – имеют специальное назначение. Признаком, по которому определяется класс IP-адреса, являются значения его нескольких первых битов. Так, адреса класса A начинаются с 0, класса B с 10, класса C со 110 и т. д. (рис. 1.30).

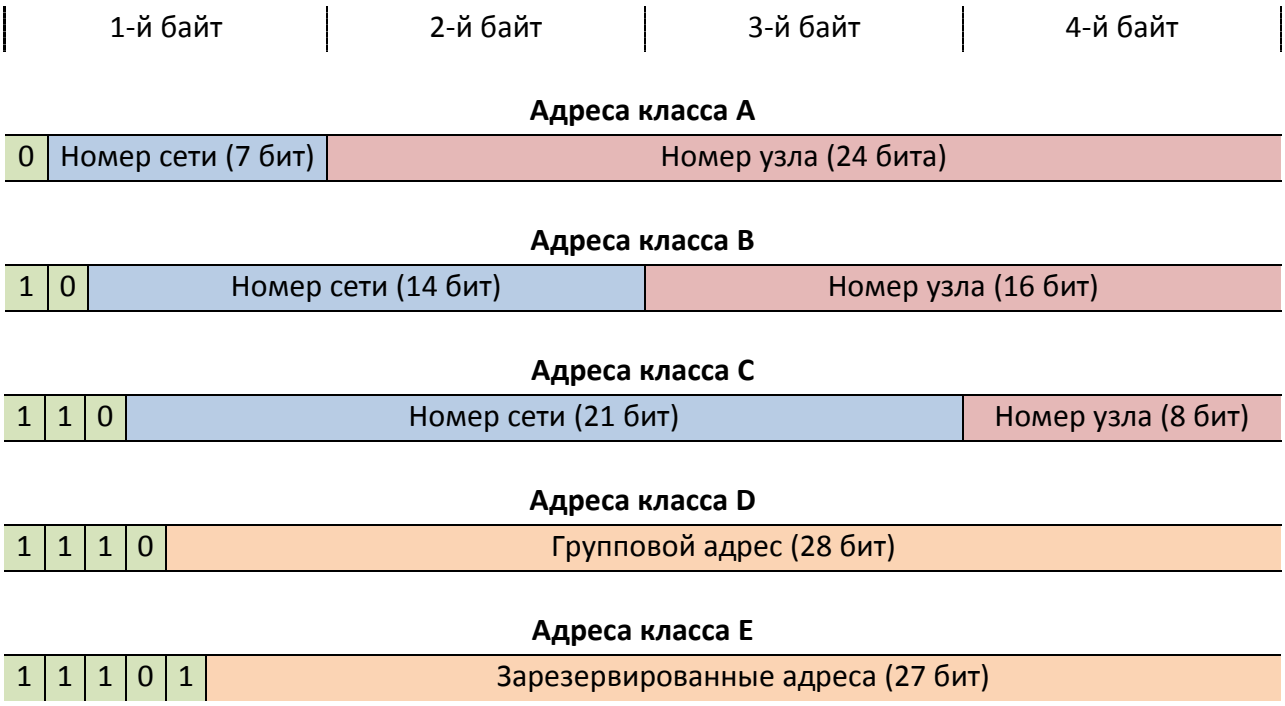


Рис. 1.30. Классы IP-адресов

Адреса класса E зарезервированы и не используются, а адреса класса D определяют группу сетевых устройств, которые могут принадлежать разным

сетям. Если при отправке данных в качестве адреса назначения указан адрес класса D, то эти данные должны быть доставлены всем узлам, которые входят в группу. По значениям первых битов адреса и по количеству битов, отводимых под номер сети и номер узла, легко определить диапазоны адресов в пределах каждого класса и посчитать максимальное количество сетей и узлов сети в каждом классе (табл. 1.4).

Таблица 1.4

Диапазоны IP-адресов

Класс адресов	Диапазон адресов в пределах класса	Максимальное количество сетей и узлов в сети класса
A	0.0.0.0 – 126.255.255.255	Сетей $2^7 - 2$, узлов $2^{24} - 2$
B	128.0.0.0 – 191.255.255.255	Сетей $2^{14} - 2$, узлов $2^{16} - 2$
C	192.0.0.0 – 223.255.255.255	Сетей $2^{21} - 2$, узлов $2^8 - 2$

Стоит отметить, что существуют ограничения при назначении IP-адресов узлам. Так номера сетей и номера узлов не могут состоять из одних двоичных нулей или единиц. Поэтому в табл. 1.4 максимальное количество сетей и узлов в сети уменьшено на 2. Кроме этого, адреса класса A, начиная с 127.0.0.0 по 127.255.255.255, не могут назначаться узлам, потому что являются зарезервированными для тестирования сетевых программ и организации работы клиентской и серверной частей приложения, установленных на одном компьютере.

Кроме этого, для обеспечения уникальности нумерации сетей и узлов в пределах каждой из сетей в стандартах Интернета определено несколько диапазонов ***частных (внутрисетевых или локальных) адресов*** предназначенных для применения в локальных сетях и не используемых в сети Интернет. К ним относятся:

- 10.0.0.0 – 10.255.255.255 в классе A;
- 172.16.0.0 – 172.31.0.0 в классе B;
- 192.168.0.0 – 192.168.255.0 в классе C.

На сегодняшний день вводятся в использование IP-адреса версии 6 (IPv6). IPv6-адрес имеет длину 128 бит и состоит из восьми групп шестнадцатеричных чисел (числа 0-9 и буквы a-f), разделенных двоеточиями. Примеры IP-адресов шестой версии:

3ffe:ffff:0000:2f3b:02aa:00ff:fe28:9c5a,

2001:0db8:85a3:08d3:1319:8a2e:0370:7334.

1.12. Доменный (символьный) адрес

Числовое представление сетевого адреса достаточно эффективно для программных и аппаратных средств. Однако пользователям удобней работать с символьными адресами.

Пространство символьных адресов Интернета разделено на области – домены. Слово домен произошло от французского domaine – область, единица структуры. В адресе каждый домен отделяется от другого точкой. Примеры различных доменных адресов: kremlin.ru, pnu.edu.ru, www.google.ru, www.microsoft.com, президент.рф, роснефть.рф[1].

Система доменных имен имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей (рис. 1.31).

Дерево имен начинается с корня, обозначаемого точкой. В доменном адресе эту точку опускают. Далее идут домены верхнего (первого) уровня, которые именуются по странам или типам организаций. Имена этих доменов должны следовать международному стандарту.

Для обозначения стран или регионов используются двухбуквенные аббревиатуры, например: ru – Россия, fr – Франция, ca – Канада, us – США, cn – Китай и т. д.

[1] .рф – национальный домен верхнего уровня для России, запущен 12 мая 2010 г., пишется кириллицей.

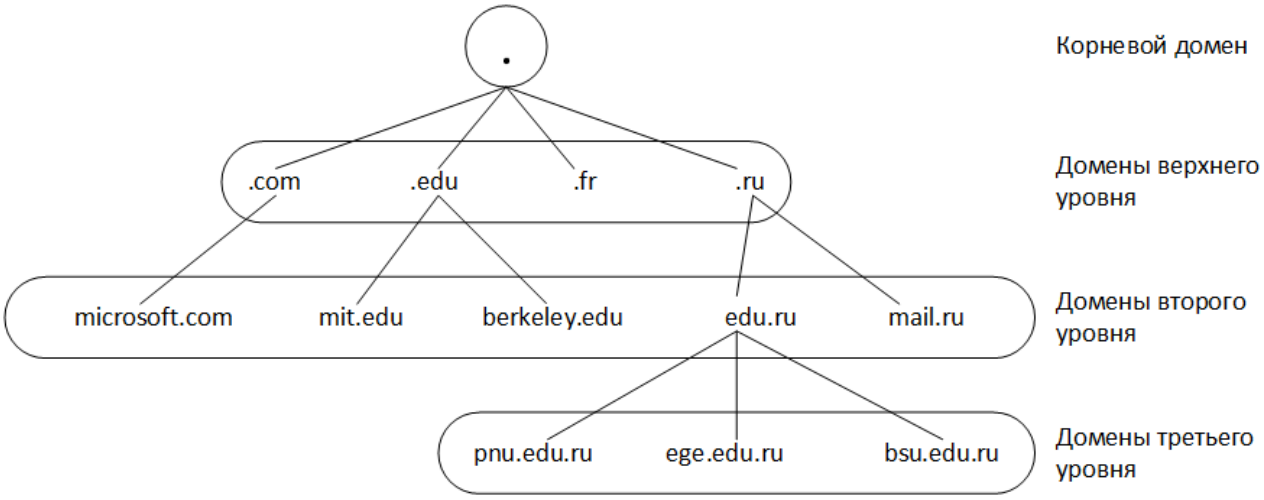


Рис. 1.31. Иерархическая структура доменных имен

Для обозначения различных типов организаций применяются, как правило, трехбуквенные сокращенные названия. Например: edu – учебные заведения США (от англ. education – образование), gov – правительственные учреждения (от англ. government – правительство), com – коммерческие организации (от англ. commercial – коммерческий), org – общественные организации (от англ. organization – организация), net – телекоммуникационные сети (от англ. network – сеть) и др.

Ниже располагаются домены второго уровня, регистрируемые в доменах верхнего уровня, и в них уже допускается регистрация как узлов, так и дочерних доменов.

Рассмотрим адрес pnu.edu.ru. Он состоит из трех доменов. Здесь домен верхнего уровня ru – домен России, домен второго уровня edu (не путать с доменом верхнего уровня edu, например, berkeley.edu или mit.edu) обозначает образовательные учреждения России, домен третьего уровня pnu (Pacific National University) относится к Тихоокеанскому государственному университету.

2. Сетевые услуги и службы

2.1. Служба World Wide Web

Служба World Wide Web (WWW, Всемирная паутина, веб-служба) предоставляет доступ к связанным между собой электронным документам, хранящимся на различных веб-серверах в сети Интернет. Эта самая популярная служба Интернета, образующая его единое информационное пространство. Отдельные электронные документы, составляющие пространство Всемирной паутины, называются ***веб-страницами*** (например, HTML-файл, содержащий ссылки на другие объекты разного типа). Группы веб-страниц, объединенных тематически, а также связанных между собой ссылками и обычно хранящихся на одном веб-сервере называют ***веб-сайтами*** (веб-узлами).

Сетевая веб-служба WWW работает по принципу клиент-сервер. ***Веб-сервер*** – это программа, хранящая веб-страницы и связанные с ними объекты в папках компьютера[1], на котором она запущена, и обеспечивающая доступ к этим объектам по URL-адресам.

Веб-клиент (браузер) представляет собой приложение, которое устанавливается на компьютере конечного пользователя и служит для загрузки и просмотра веб-страниц. Одной из важных функций браузера является поддержка пользовательского графического интерфейса для поиска, просмотра веб-страниц, навигации между уже просмотренными страницами, хранения истории посещений. Помимо этого, веб-браузер предоставляет пользователю возможность манипулирования страницами: сохранение их в файле на диске своего компьютера, печать на принтере, поиск информации в пределах страницы, добавление страницы в закладки, изменение кодировки, просмотр исходного кода и др.

[1] Как говорилось ранее, под сервером понимается также и компьютер, с установленным на нем серверным программным модулем.

URL-адрес

В сети Интернет адреса имеют как узлы сети, так и отдельные ресурсы (чаще всего веб-страницы и файлы на серверах). Для доступа к таким ресурсам используются адреса специального формата, называемые URL (Uniform Resource Locator – унифицированный указатель ресурса). Примеры URL-адресов:

http://www.olifer.co.uk/books/books.htm

http://www.itu.int/ru/pages/default.aspx

http://pnu.edu.ru/ru/faculties/full_time/fkfn/

В типичном URL-адресе можно выделить три части (рис. 2.1):

1. Сетевой протокол. Протоколом доступа к веб-страницам является HTTP, но могут быть указаны и другие протоколы, например, FTP.

2. Доменное имя сервера, на котором хранится ресурс.

3. Путь к ресурсу – имя папки (вложенных папок) и файла на сервере.

$$\underbrace{\text{http://}}_{\text{протокол}}\ \underbrace{\text{www.starline.org}}_{\text{DNS–имя сервера}}\ /\ \underbrace{\text{company/about.htm}}_{\text{путь к ресурсу}}$$

Рис. 2.1. Структура URL-адреса

В примере рис. 2.1 доступ к ресурсу на сервере www.starline.org осуществляется по протоколу HTTP. Сам ресурс – файл about.htm – располагается в папке company корневого каталога сервера. По расширению можем сделать вывод о том, что это HTML-файл.

Протокол HTTP

Веб-клиент и веб-сервер взаимодействуют друг с другом по протоколу HTTP (Hypertext Transfer Protocol – протокол передачи гипертекста). Согласно протоколу, обмен сообщениями проходит по схеме «запрос-ответ». Веб-сервер постоянно находится в активном состоянии. Как только сервер полу-

чает запрос от клиента, он устанавливает соединение и получает от клиента имя объекта и путь к нему, например, «company/about.htm» (рис. 2.2). После этого сервер находит указанный файл и отсылает его клиенту. Получив объекты от сервера, веб-браузер отображает их на экране.

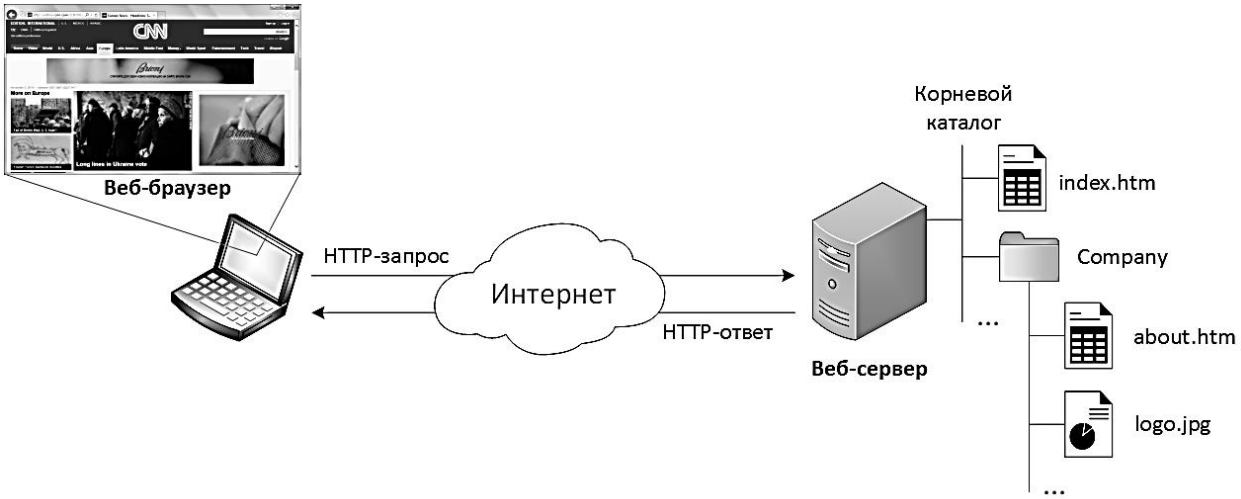


Рис. 2.2. Работа протокола HTTP

Для защиты передаваемых по протоколу HTTP данных используется расширение этого протокола – HTTPS (Hypertext Transfer Protocol Secure), поддерживающее шифрование.

2.2. Передача файлов по протоколу FTP

Протокол передачи файлов FTP (File Transfer Protocol) обеспечивает способ перемещения файлов с удаленного компьютера на локальный и наоборот. Является одним из старейших прикладных протоколов, появился в 1971 г. задолго до HTTP. До появления веб-службы сетевая файловая служба на основе протокола FTP долгое время была самой популярной службой доступа к удаленным данным в Интернете.

Протокол построен по принципу клиент-сервер. Программные модули FTP-сервера и FTP-клиента имеются практически в каждой операционной системе, кроме этого FTP-клиенты встроены в веб-браузеры, которые могут из-

влекать файлы, расположенные на FTP-серверах. На рис. 2.3 показано окно веб-браузера с содержимым FTP-сервера компании Redcom.

Рис. 2.3. Содержимое FTP-сервера компании Redcom

Имеются расширения протокола FTPS и SFTP, предназначенные для безопасной передачи файлов.

2.3. Электронная почта

Электронная почта (email от англ. electronic mail) – это одна из самых популярных услуг в компьютерных сетях. Как и обычная, электронная почта является асинхронным средством связи: люди посылают друг другу сообщения в любое удобное для них время без предварительной договоренности с адресатами. Преимуществами электронной почты являются высокая скорость доставки, простота и мобильность использования, низкая стоимость обслуживания. С помощью списка рассылки с адресами отправитель может разослать одно и то же письмо сотням получателей одновременно. Кроме того, электронная почта позволяет вместе с текстом письма пересылать изображения, аудио-, видео- и другие типы файлов.

Каждый пользователь электронной почты обладает собственным почтовым ящиком, расположенным на почтовом сервере. Адрес почтового ящика состоит из имени пользователя и доменного имени сервера, разделенных символом «@» (в разговорном языке «собака»):

пользователь@домен.

Например, ivanov@pochta.com. Символ «@» в английском языке означает сокращенный предлог at – указание на местоположение, предлоги «в», «у», «на». Поэтому ivanov@pochta.com следует понимать как «ivanov на почтовом сервере pochta.com». В адресе электронного почтового ящика допускаются только буквы английского алфавита, цифры, точка, минус и знак подчеркивания. Заглавные и строчные буквы в адресе не различаются.

В почтовом ящике хранятся все сообщения, адресуемые пользователю. Как правило, обычные пользователи используют для создания почтовых ящиков почтовый сервер своего Интернет-провайдера или бесплатные почтовые сервисы такие как, Gmail, Почта@mail.ru, Яндекс.Почта и др. в предлагаемом домене (@gmail.com, @mail.ru, @inbox.ru, @yandex.ru и т. д.). В крупных компаниях для организации корпоративной почты часто используют собственный почтовый сервер с доменным именем, обозначающим принадлежность этой компании, или платные почтовые сервисы также с собственным доменным именем.

Рассмотрим технологию работы и протоколы прикладного уровня, составляющие основу электронной почты. Существует два способа работы пользователя с электронной почтой: через программу почтового клиента (например, Microsoft Outlook, The Bat, Mozilla Thunderbird и др.), рис. 2.4 и через веб-интерфейс, рис. 2.5. В обоих случаях пользователи обрабатывают электронные сообщения с помощью своих персональных компьютеров или мобильных устройств, а почтовые серверы используются для отправки, получения и хранения почты.

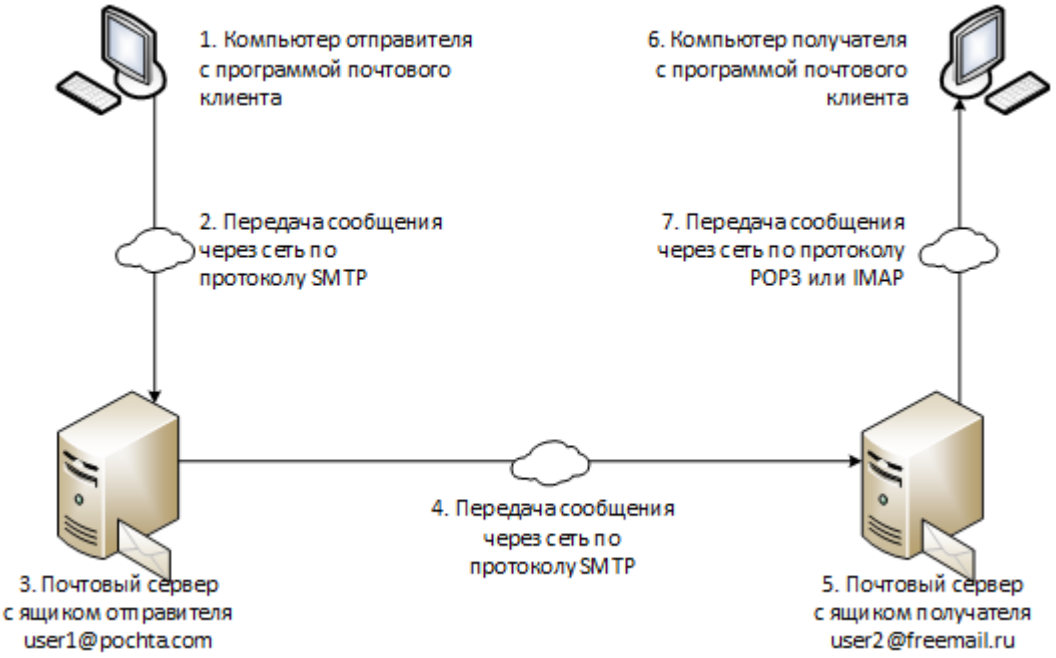


Рис. 2.4. Схема работы электронной почты через программу почтового клиента

Работа электронной почты через программу почтового клиента:

1. Отправитель на своем компьютере запускает установленную на нем программу почтового клиента. В этой программе он печатает текст электронного письма, указывает адрес получателя «user2@freemail.ru», необходимую сопроводительную информацию (тему письма, отметку о срочности доставки, подтверждении факта прочтения этого письма) и нажимает кнопку «отправить».

2. Почтовый клиент устанавливает соединение с почтовым сервером домена «pochta.com», к которому относится почтовый ящик отправителя «user1@pochta.com», и отсылает ему электронное письмо по протоколу SMTP. SMTP является протоколом отправки (англ. pull protocol), в котором клиент является инициатором передачи данных на сервер.

3. Письмо, попав на почтовый сервер отправителя, помещается для хранения в почтовый ящик отправителя «user1@pochta.com» и помещается в очередь исходящих сообщений.

4. SMTP-клиент, выполняющийся на почтовом сервере отправителя, обнаруживает сообщение в очереди, по указанному адресу

«user2@freemail.ru» определяет почтовый сервер получателя, устанавливает с ним соединение и отправляет письмо по протоколу SMTP.

5. Сервер «freemail.ru» принимает переданное сообщение и по окончанию приема помещает его в почтовый ящик получателя «user2@freemail.ru».

6. Получатель в удобное ему время, которое не связано с моментом поступления сообщения на сервер, запускает на своем компьютере почтовую программу и выполняет команду проверки почты.

7. После этой команды почтовый клиент должен запустить протокол доступа к почтовому серверу. Т. к. протокол SMTP используется для передачи данных от клиента на сервер, то на данном шагее применяется другой протокол – протокол приема данных (англ. push protocol). В нем клиент является инициатором получения данных от сервера. К таким протоколам доступа к почтовому серверу относятся POP3 (Post Office Protocol Version 3 – протокол почтового отделения, версия 3) и IMAP (Internet Mail Access Protocol – протокол доступа к почте Интернета). В результате работы любого из них письмо отправителя оказывается в памяти компьютера получателя.

В сравнении с IMAP протокол POP3 более простой и имеет некоторые ограничения: не позволяет пользователю организовать почту на сервере, создавая различные папки, а также частично проверить содержание почты перед загрузкой. Кроме того, в режиме удаления протокола POP3 письмо, попав в компьютер пользователя, удаляется из почтового сервера. Если пользователь имеет доступ к почтовому ящику с разных устройств, то на них будет различная почта. В этом случае необходим режим сохранения.

При доступе к электронной почте через веб-интерфейс роль программы почтового клиента играет веб-браузер, который взаимодействует с удаленным потовым ящиком по протоколу HTTP, а не SMTP, IMAP или POP3 (рис. 2.5). Обмен сообщениями между почтовыми серверами отправителя и получателя, как и ранее, происходит по протоколу SMTP.

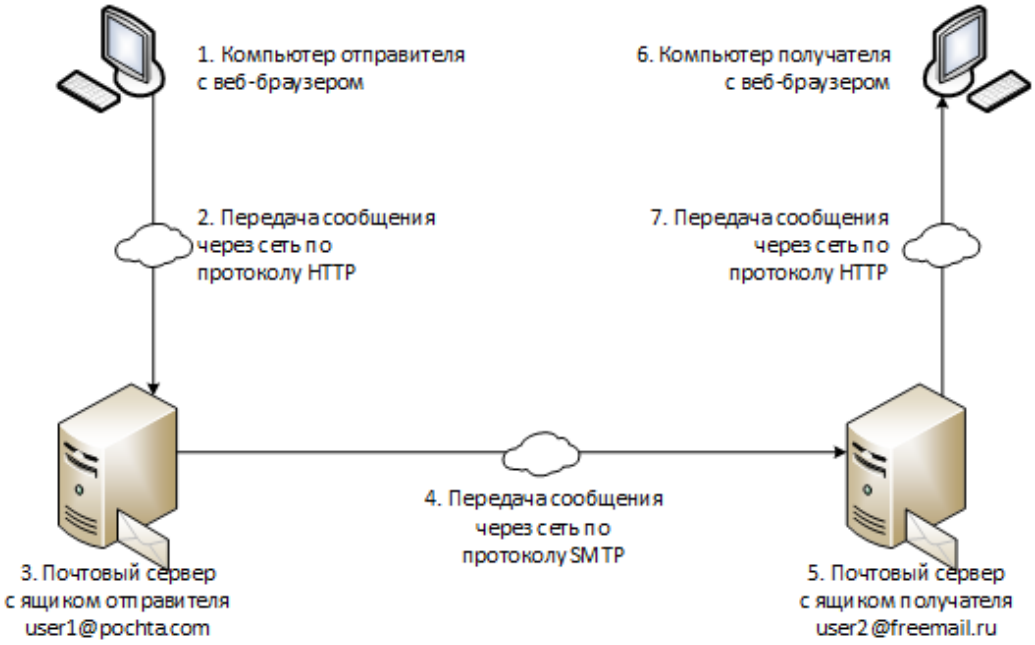


Рис. 2.5. Работа с электронной почтой через веб-интерфейс

2.4. Служба трансляции имен Интернета

В сети Интернет символьные и цифровые адреса применяются одновременно. Между доменным именем и IP-адресом, относящимся к одному и тому же сетевому узлу, нет никакой функциональной зависимости. Компьютеры, имена которых относятся к одному и тому же домену, могут иметь абсолютно независимые друг от друга IP-адреса. В процессе передачи данных доменный адрес преобразуется в IP-адрес.

Установлением соответствия между символьными именами и цифровыми адресами занимается служба ***DNS – система доменных имен*** (Domain Name System). В сети выделяются специальные компьютеры, называемые серверами имен или DNS-серверами, на которых хранятся таблицы соответствия друг другу доменного имени и IP-адреса. Например:

pnu.edu.ru – 85.142.70.252

ege.edu.ru – 62.76.166.20

Таким образом, DNS представляет собой, с одной стороны, распределенную между серверами имен базу данных, а с другой – протокол прикладного уровня, организующий взаимодействие между компьютерами и серве-

рами имен для выполнения операций преобразования. Обычно DNS используется другими протоколами прикладного уровня, такими как HTTP, FTP и SMTP, для получения IP-адресов вместо вводимых пользователем символьных адресов. Например, пользователь вводит в адресной строке браузера адрес веб-страницы www.starline.org/company/about.htm. Для того чтобы сформировать http-запрос к веб-серверу, на котором находится указанный ресурс, браузер вначале с помощью протокола DNS получает IP-адрес этого сервера по доменному имени из URL-адреса www.starline.org. После этого устанавливается соединение с веб-сервером.

2.5. Облачные вычисления

На сегодняшний день одним из самых активно развивающихся и внедряющихся в различные сферы деятельности направлений сетевых услуг являются облачные технологии.

Под ***облачными технологиями*** (или облачными вычислениями от англ. cloud computing) понимают технологии распределенной обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис. Облачные вычисления представляют собой результат эволюции и объединения множества различных технологий, которые изменили организационный подход к построению информационной инфраструктуры предприятия.

Облачные сервисы подразделяются на программные сервисы и сервисы инфраструктуры. В настоящее время сложилось три модели использования сервисов облачных вычислений:

1. Infrastructure as a Service (IaaS) – инфраструктура как сервис. IaaS предлагает доступ к низкоуровневым ресурсам: хранилищам данных, вычислительным устройствам и памяти. Примерами являются хранилища Amazon S3, SQL Azure, вычисления Amazon EC2, Elastichosts.

2. Platform as a Service (PaaS) – платформа как сервис. Платформа – это прикладной программный интерфейс, обеспечивающий приложению возможность работы в условиях «облака». Приложение работает под управлением специализированной операционной системы, предоставляемой поставщиком облачных вычислений. IaaS может только гарантировать определенное количество процессоров или объем памяти, а все остальное должно делать размещаемое пользователем приложение. Примеры: Force.com, Google App Engine, Microsoft Azure (Platform).

3. Software as a Service (SaaS) – приложение как сервис. Представляет собой модель развертывания программного обеспечения на основе Web, благодаря чему оно полностью доступно через веб-браузер без установки дополнительного ПО. Примеры: Google Apps, MS Office 365, Apple iCloud.

На рис. 2.6 в виде перевернутой пирамиды представлены перечисленные модели облачных услуг. Больший размер блока пирамиды означает, что он включает в себя всю инфраструктуру меньшего блока. Например, для предоставления сервиса PaaS с точки зрения поставщика услуг необходимо также иметь возможность обеспечить сервис IaaS. Каждая из представленных моделей имеет свою целевую аудиторию, которая приведена справа.

Рис. 2.6. Модели облачных услуг

3. Безопасность в компьютерных сетях

3.1. Понятие безопасной связи

Рассмотрим модель сетевого взаимодействия двух участников (абонентов). В литературе по защите информации их принято обозначать английским буквами A и B, и называть именами Алиса и Боб соответственно. В качестве таких участников сетевого взаимодействия могут выступать обычные пользователи на конечных узлах (например, желающие обменяться письмами по электронной почте), программные модули (например, веб-браузер и веб-сервер) или аппаратные устройства (например, маршрутизаторы, обменивающиеся таблицами маршрутизации в системе DNS).

Алиса отправляет некоторое сообщение (информационное или управляющее) Бобу по открытому информационному каналу связи (рис. 3.1). Открытый канал связи подразумевает доступность для прослушивания другим лицам, отличным от отправителя Алиса и получателя Боба. Обычно «другим лицом» является злоумышленник E, целью которого является нанесение вреда абонентам.

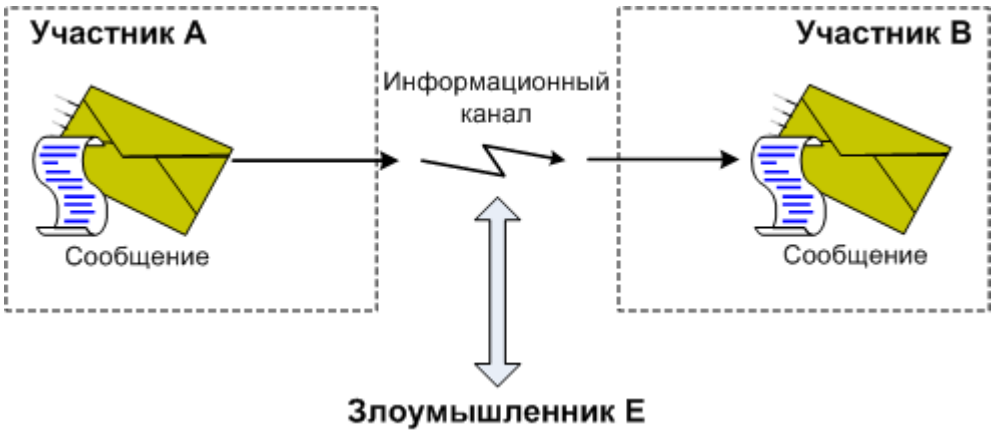


Рис. 3.1. Передача сообщения

Для того чтобы сетевое взаимодействие между абонентами было безопасным, должны выполняться следующие свойства:

– ***конфиденциальность*** – гарантия того, что только отправитель и предполагаемый получатель способны понять содержимое передаваемых сообщений. Поскольку злоумышленники могут перехватывать сообщения, они должны быть зашифрованы;

– ***аутентификация*** – подтверждение того, что информация получена из законного источника, и получатель действительно является теми, за кого себя выдает.

– ***целостность данных*** – гарантия того, что информация при хранении или передаче не изменилась (случайно или намеренно);

– ***управление доступом*** – гарантия того, что пользователи, пытающиеся получить доступ к ресурсам, смогут сделать это только в том случае, если обладают соответствующими правами доступа и осуществляют этот доступ определенным образом.

Для обеспечения данных свойств безопасной связи применяются различные механизмы и сервисы безопасности, которые представляют собой программные и программно-аппаратные средства (например, программы или устройства для шифрования, протоколы обмена сообщениями и др.).

3.2. Классификация сетевых атак

Атакой называется любое действие, нарушающее безопасность информационной системы. Атаки по определению являются умышленными и обычно квалифицируются как преступления. Как правило, атака предваряется выявлением слабых мест в системе – ***уязвимостей***, сбором дополнительной информации о системе, которая позволяет эффективно спланировать атаку и скрыть следы проникновения в систему.

Все атаки, предпринимаемые злоумышленниками в сети, можно разделить на два класса: пассивные и активные.

Пассивной называется такая атака, при которой злоумышленник не имеет возможности изменять передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения (рис. 3.2). Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ сетевого трафика.

Рис. 3.2. Схема пассивной атаки

Анализ трафика – это изучение параметров передаваемых данных (не содержимого, а их характеристик):

– кто с кем общается;

– когда общается;

– насколько длинные сообщения;

– как быстро посылаются ответы и насколько они длинные;

– какого рода связь возникает после получения определенного сообщения и другие.

Ответы на подобные вопросы могут быть очень информативными для злоумышленника.

Наоборот, ***активной*** называется такая атака, при которой злоумышленник может модифицировать передаваемые по информационному каналу сообщения и вставлять свои. Различают следующие четыре типа активных атак.

Создание ложного потока (фальсификация, нарушение аутентичности) означает попытку одного субъекта выдать себя за другого (рис. 3.3).

Рис. 3.3. Создание ложного потока

Повторное использование (replay-атака) означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа (рис. 3.4). Replay-атаки являются одним из вариантов фальсификации, но так как это один из наиболее распространенных вариантов атаки для получения несанкционированного доступа, его часто рассматривают как отдельный тип.

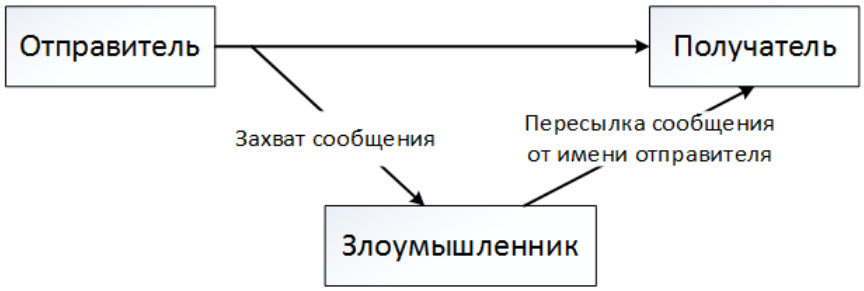


Рис. 3.4. Replay-атака

Модификация потока данных («человек посередине», англ. «man in the middle») означает либо изменение злоумышленником содержимого пересылаемого сообщения, либо изменение порядка сообщений (рис. 3.5).

Рис. 3.5. Атака «человек посередине»

Отказ в обслуживании (DoS-атака, англ. Denial of Service) нарушает нормальное функционирование сетевых сервисов. Такие атаки направляются обычно на информационные серверы предприятия, функционирование которых является критически важным условием для работоспособности всего предприятия. Злоумышленник, захватив управление над группой удаленных компьютеров, координируют их работу[1] (как правило, без ведома пользователей этих компьютеров), «заставляет» их посылать запросы в адрес узла-жертвы (рис. 3.6). Получившийся в результате мощный суммарный поток перегружает атакуемый компьютер и, в конечном счете, делает его недоступным. Блокировка происходит в результате исчерпания ресурсов либо процессора, либо операционной системы, либо канала связи.

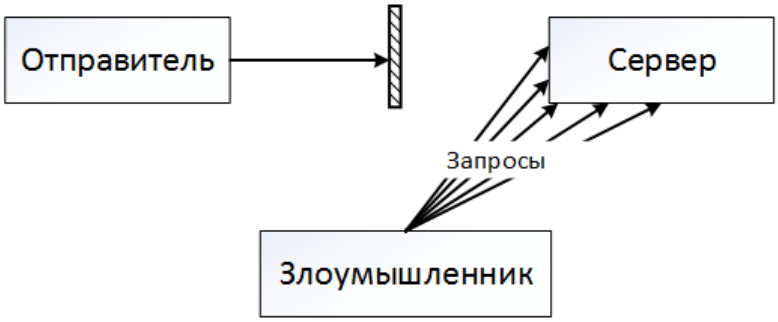


Рис. 3.6. DoS-атака

3.3. Шифрование

Для того чтобы злоумышленник не смог получить информацию из передаваемого по сети сообщения, его нужно сделать секретным – зашифровать (рис. 3.7).

Наука о методах обеспечения конфиденциальности информации называется ***криптографией***. Криптографические методы шифрования позволяют отправителю скрыть содержимое своих посланий, поэтому злоумышленник не может получить информацию из перехваченных сообщений.

[1] Говорят, что в таких случаях имеет место распределенная атака отказа в обслуживании (Distributed Denial of Service, DDoS).

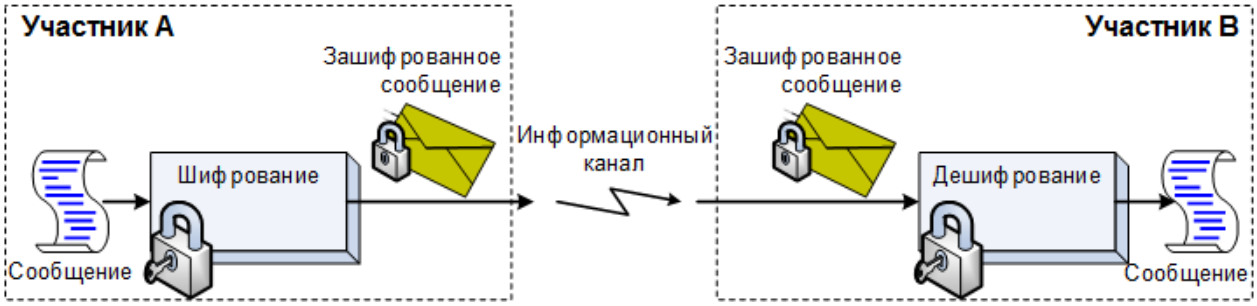


Рис. 3.7. Передача зашифрованного сообщения

Вы, не подозревая того, часто используете криптографические средства защиты данных, когда отправляете письмо по электронной почте, совершаете покупку через Интернет-магазин, работаете с банковским счетом через онлайн банкинг и т. д.

Проблема шифрования информации имеет долгую историю. Известен шифр, изобретенный Гаем Юлием Цезарем, в котором каждая буква сообщения заменялась другой, стоящей тремя буквами правее по алфавиту: то есть A заменялась на D, B на E, C на F и так далее. Три последние буквы алфавита X, Y, Z шифровались тремя первыми A, B, C. Так слово HELLO превращается в зашифрованное слово KHOOR.

Очень долго шифрование использовалось в основном в военных и политических целях. Сегодня с развитием вычислительной техники и информационных технологий криптографические методы защиты данных стали применяться очень широко, обслуживая, в первую очередь, потребности бизнеса.

Криптографические алгоритмы шифрования используются для обеспечения конфиденциальности хранимых или передаваемых данных. Алгоритмы с помощью определенных правил преобразуют исходные данные в зашифрованный вид так, чтобы восстановить эти данные мог только законный пользователь. Этот процесс называется ***шифрованием***. Для получения исходной информации необходимо над зашифрованным текстом выполнить обратный процесс преобразования – ***дешифрование***. При шифровании и дешифровании данных обычно применяется сменный элемент алгоритма,

называемый в криптографии ***ключом***. Считается, что злоумышленник может знать использованный алгоритм шифрования, характер передаваемых сообщений и перехваченный зашифрованный текст, но не знает секретный ключ.

Исходное сообщение, отправляемое Алисой, называется ***открытым текстом*** и обозначается буквой M (от англ. message). Это может быть текстовый файл, цифровое изображение, звук или видео – все равно. Для компьютера – это просто набор бит. Зашифрованное с помощью некоторого алгоритма сообщение называется ***шифротекстом*** и обозначается буквой C (от cipher text).

Существуют два основных типа криптографических алгоритмов: алгоритмы симметричного шифрования и алгоритмы шифрования с открытым ключом. Рассмотрим каждый тип подробнее.

Алгоритмы симметричного шифрования

В ***симметричных алгоритмах*** для шифрования и дешифрования сообщений используется один общий для участников секретный ключ K_{AB}. Схема такого шифрования приведена на рис. 3.8.

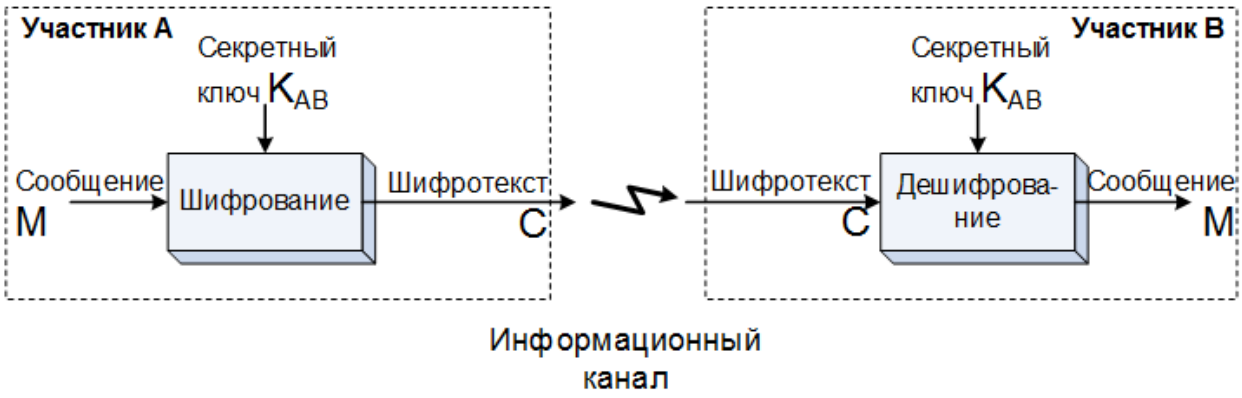


Рис. 3.8. Схема симметричного шифрования

Рассмотрим, как происходит обмен информацией.

1. Для начала Алиса и Боб выбирают алгоритм шифрования.

2. Далее оба выбирают секретный ключ K_{AB}.

3. Алиса шифрует с помощью алгоритма и секретного ключа K_{AB} свое сообщение, получая шифротекст С.

4. Затем она посылает шифрованное сообщение Бобу.

5. Боб, получив шифротекст, дешифрует его с помощью этого же алгоритма и секретного ключа K_{AB}. Теперь он может прочитать открытый текст сообщения.

Симметричный алгоритм можно представить в виде дипломата с кодовой комбинацией. Тогда комбинация будет секретным ключом. Алиса, зная ее, открывает дипломат, кладет в него документ, закрывает и отправляет его Бобу. Тот, в свою очередь, зная эту же кодовую комбинацию, открывает дипломат и получает документ.

Наиболее известными алгоритмами симметричного шифрования являются алгоритм стандарта США AES (Advanced Encryption Standard), алгоритм российского стандарта ГОСТ 28147-89, алгоритм DES и 3DES, RC6, Blowfish, IDEA и др.

К достоинствам симметричных алгоритмов относятся достаточно быстрая скорость работы и возможность аппаратной реализации. Однако, при использовании систем шифрования с симметричным ключом сложностью является передача секретного ключа защищенным способом от одного абонента другому, чтобы злоумышленник не смог перехватить этот ключ. Несимметричные алгоритмы, основанные на использовании открытых ключей, снимают эту проблему.

Алгоритмы шифрования с открытым ключом

В отличие от симметричных алгоритмов в ***алгоритмах шифрования с открытым ключом*** используются два ключа: открытый (или еще называемый публичным) ключ K^+ для шифрования и личный (секретный) ключ K^- для дешифрования сообщений (рис. 3.9).

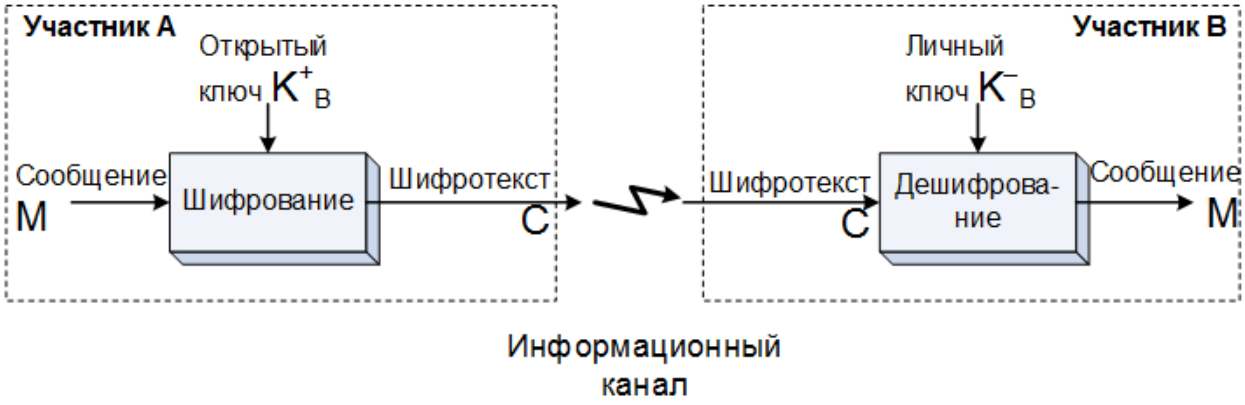


Рис. 3.9. Схема шифрования с открытым ключом

Рассмотрим данную схему шифрования подробнее.

1. Алиса и Боб согласовывают алгоритм шифрования.

2. Боб генерирует два ключа: открытый ключ K_B^+ и личный ключ K_B^-.

3. Дальше Боб делает свой открытый ключ доступным Алисе. Можно опубликовать его на сайте, поместить в общедоступную базу данных ключей, отправить по электронной почте или передать лично. В любом случае ключ передается в незащищенном виде, так как расшифровать сообщение можно будет только с помощью личного ключа.

4. Алиса шифрует с помощью алгоритма и открытого ключа Боба K_B^+ свое сообщение, получая шифротекст С.

5. Она посылает шифрованное сообщение Бобу.

6. Боб дешифрует шифротекст с помощью этого же алгоритма, но с использованием уже личного ключа K_B^-.

Как видно из третьего шага, открытый ключ может быть известен всем: кто угодно может использовать его для шифрования сообщений, но только конкретный абонент с соответствующим личным ключом может расшифровать эти сообщения. Такой алгоритм легко сравнить с почтовым ящиком. Каждый желающий может опустить в него письмо. Это аналогично шифрованию. Дешифрование представляет собой извлечение почты из ящика, открыв его с помощью ключа.

Наиболее известными алгоритмами шифрования с открытым ключом являются RSA, Rabin, шифр Эль-Гамаля.

В отличие от симметричных криптосистем алгоритмы с открытым ключом работают медленнее и требуют бо́льших вычислительных ресурсов. Поэтому на практике асимметричные криптосистемы часто используются в сочетании с другими алгоритмами (симметричными, хеш-функциями).

Для того чтобы абоненты в сети могли принимать зашифрованные сообщения, каждый должен сгенерировать свою пару ключей. Хотя информация об открытом ключе не является секретной, ее нужно защищать от подлогов, чтобы злоумышленник не смог применить атаку фальсификации: под именем легального пользователя передать свой открытый ключ, после чего расшифровывать все сообщения, посылаемые легальному пользователю, и отвечать от его имени. Решением этой проблемы является технология цифровых сертификатов.

Сертификат представляет собой электронный документ, который связывает конкретного пользователя с конкретным ключом. В сертификате содержатся сведения о владельце сертификата, такие как имя, адрес электронной почты; значение открытого ключа владельца данного сертификата; срок действия сертификата (время, в течение которого сертификат считается действительным); наименование сертифицирующей организации, выдавшей данный сертификат и др.

Цифровые сертификаты бывают разных классов, отличающихся уровнем полномочий, которые получает его владелец. Например, сертификаты компании Verisign бывают пяти классов. Первый класс предоставляет пользователю самый низкий уровень полномочий и может использоваться для защиты электронной почты, а сертификаты четвертого и пятого класса используются при выполнении крупных финансовых операций и транзакций между компаниями.

Просмотреть имеющиеся на компьютере с операционной системой Windows сертификаты можно с помощью меню Пуск → Панель управления → Свойства браузера → вкладка Содержание → Сертификаты (рис. 3.10).

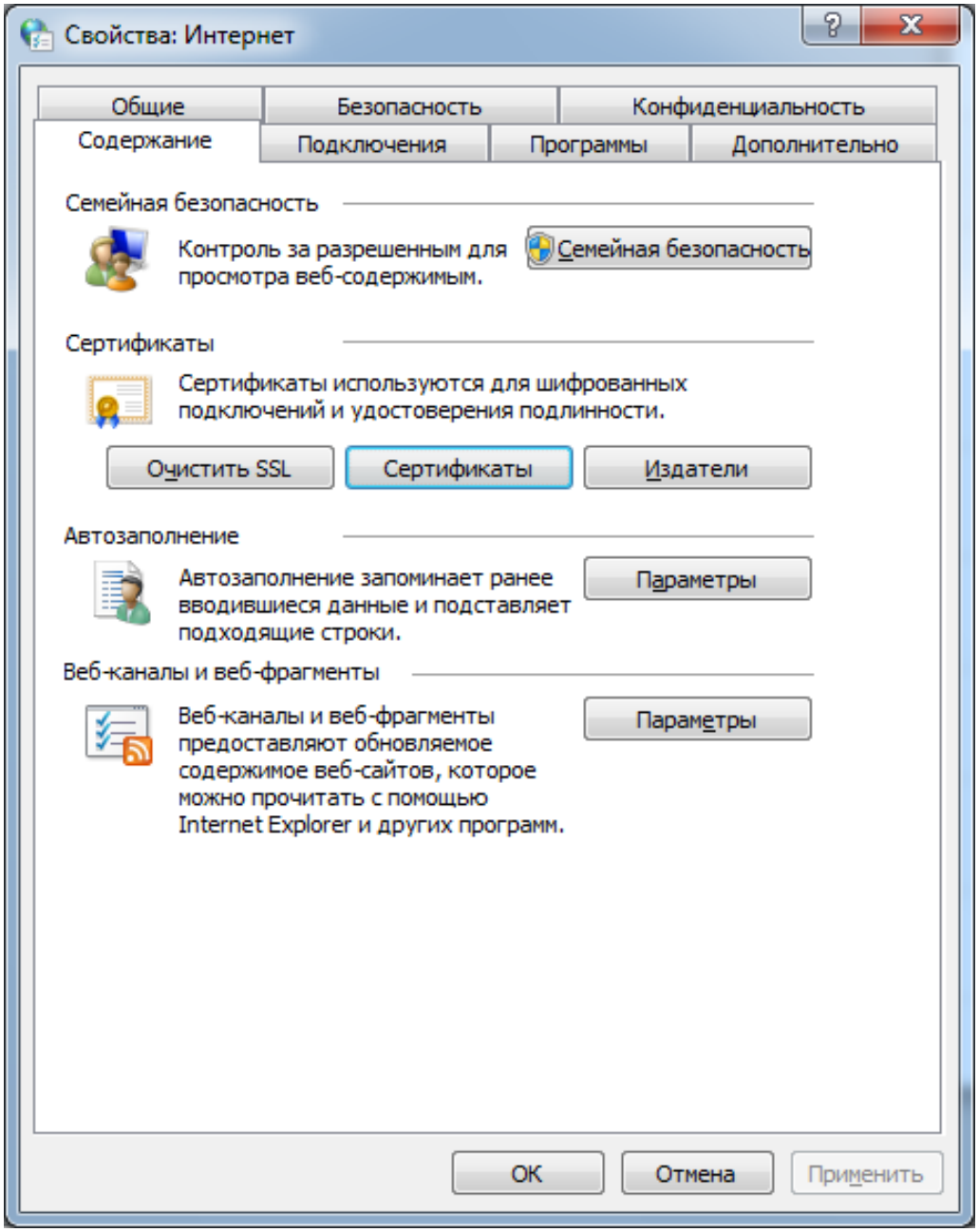


Рис. 3.10. Вкладка «Содержание» окна «Свойства браузера»

Сертификаты хранятся в файлах специального формата, имеющих расширения .crt, .cer, .p7r, .p7b. На рис. 3.11 представлено окно с содержимым одного из сертификатов.

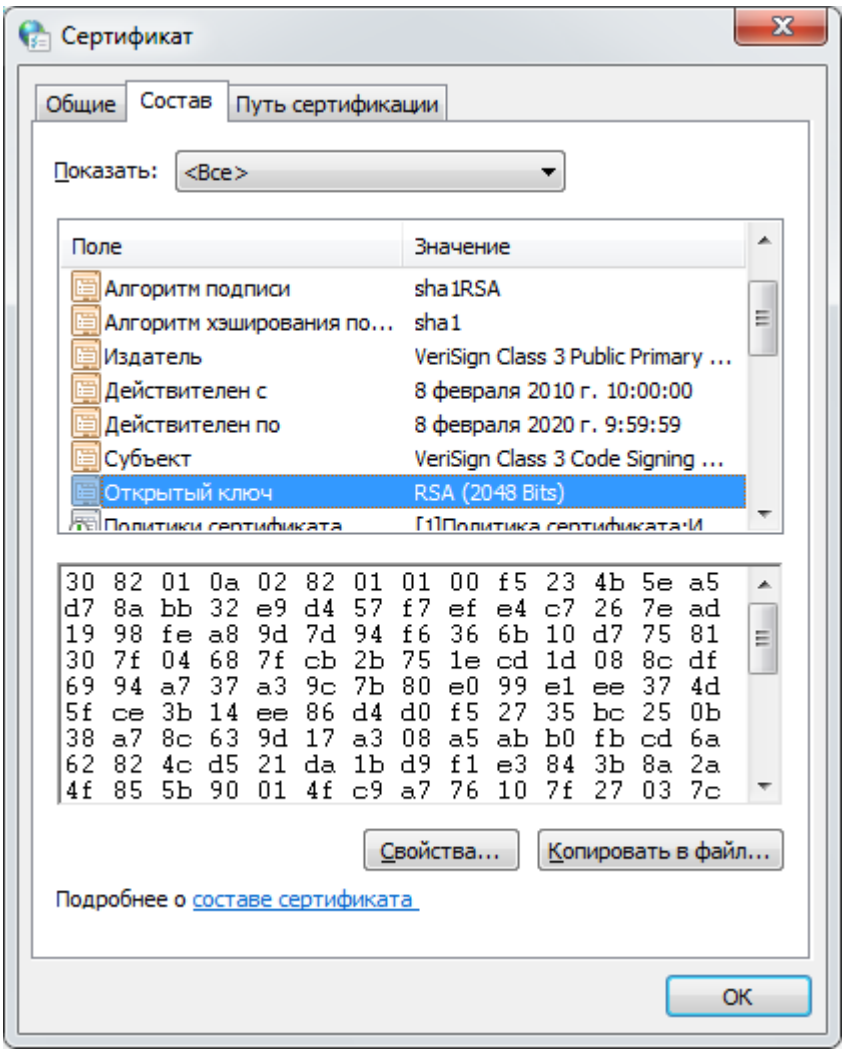


Рис. 3.11. Содержимое сертификата

3.4. Электронная цифровая подпись

Мы привыкли ставить рукописную подпись на важных документах. Однако существует электронная цифровая подпись (ЭЦП), которая применяется к электронным документам и сохраняет свойства обычной рукописной подписи:

– удостоверяет, что подписанный документ исходит от лица, поставившего подпись;

– не дает лицу, подписавшему документ, отказаться от обязательств;

– гарантирует целостность подписанного документа.

В России действует федеральный закон «Об электронной цифровой подписи», обеспечивающий правовые условия использования электронной

цифровой подписи, и ГОСТ Р 34.10–2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», описывающий алгоритмы формирования и проверки ЭЦП».

Предположим, участник хочет снабдить электронной цифровой подписью отправляемое сообщение. Здесь на помощь приходят алгоритмы шифрования с открытым ключом, которые имеют следующее замечательное свойство. Шифровать сообщение можно используя личный ключ, а дешифровать, используя открытый. Тогда:

1. Боб шифрует сообщение M своим личным ключом K_B^-, таким образом, подписывая его.

2. Боб посылает исходное сообщение M и подпись $K_B^-(M)$ Алисе.

3. Алиса расшифровывает подпись $K_B^-(M)$, используя открытый ключ Боба K_B^+. Успешное сравнение расшифрованной подписи с исходной версией сообщения M будет означать, что документ действительно подписан Бобом.

Проверить соответствие значения $K_B^-(M)$ документу M может кто угодно, но сгенерировать $K_B^-(M)$ может только участник В с помощью своего личного ключа, что и требуется для подписи.

В данном случае участник для создания цифровой подписи шифрует сообщение M целиком. Подобное шифрование может потребовать массы вычислительных ресурсов и времени. Более эффективный подход состоит в вычислении так называемого дайджеста сообщения.

Дайджест сообщения (хеш-код, «отпечаток пальца» сообщения) – это строка бит фиксированной длины, которая вычисляется из сообщения с помощью хеш-функции.

Хеш-функция представляет собой однонаправленную криптографиче-

скую функцию H, которая применяется к сообщению M произвольной длины и возвращает значение h фиксированной длины (рис. 3.12).

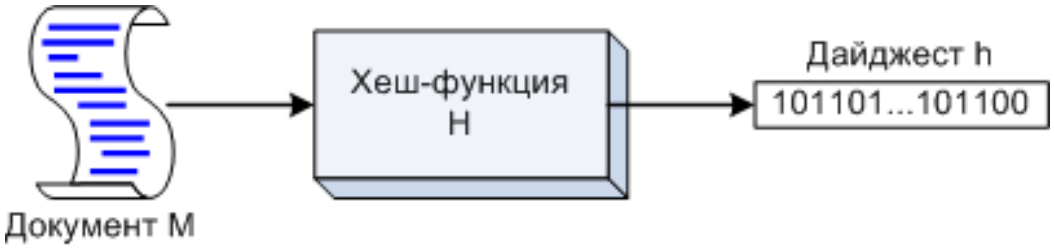


Рис. 3.12. Схема хеш-функции

Основные требования, которые предъявляются к криптографическим хеш-функциям:

1. Для любого M вычисление $H(M)$ должно выполняться относительно быстро.

2. При известном h должно быть трудно (практически невозможно) найти M, для которого $h = H(M)$.

3. При известном сообщении M должно быть трудно найти другое сообщение $M' \neq M$, такое, что $H(M') = H(M)$.

4. Должно быть трудно найти какую-либо пару различных сообщений M и M', для которых $H(M') = H(M)$.

Первые два требования устанавливают однонаправленность хеш-функции: легко вычислить значение хеш-функции h по сообщению M, но трудно получить сообщение M, зная только значение h. Знание дайджеста не дает возможности восстановить исходное сообщение, но зато позволяет проверить целостность данных. Четвертое требование является более сильным, чем третье (т. е. при выполнении четвертого автоматически выполняется и третье).

Хеш-функции используются также для необратимого шифрования паролей. В большинстве случаев парольные фразы не хранятся в исходном виде,

а хранятся лишь их хеш-коды. Хранить исходные пароли небезопасно, поскольку злоумышленник может получить к ним доступ, а при хранении хеш-значений он не сможет обратить их в первоначальный вид. В ходе процедуры проверки введенного пользователем пароля вычисляется его хеш-код и сравнивается с сохранённым.

В настоящее время предложены и практически используются хеш-функции MD5, SHA-1, SHA-256, SHA-512, RIPEMD-160, алгоритм российского стандарта ГОСТ Р 34.11–2012 и др.

Теперь с использованием хеш-функции процесс подписи документа будет выглядеть так (рис. 3.13).

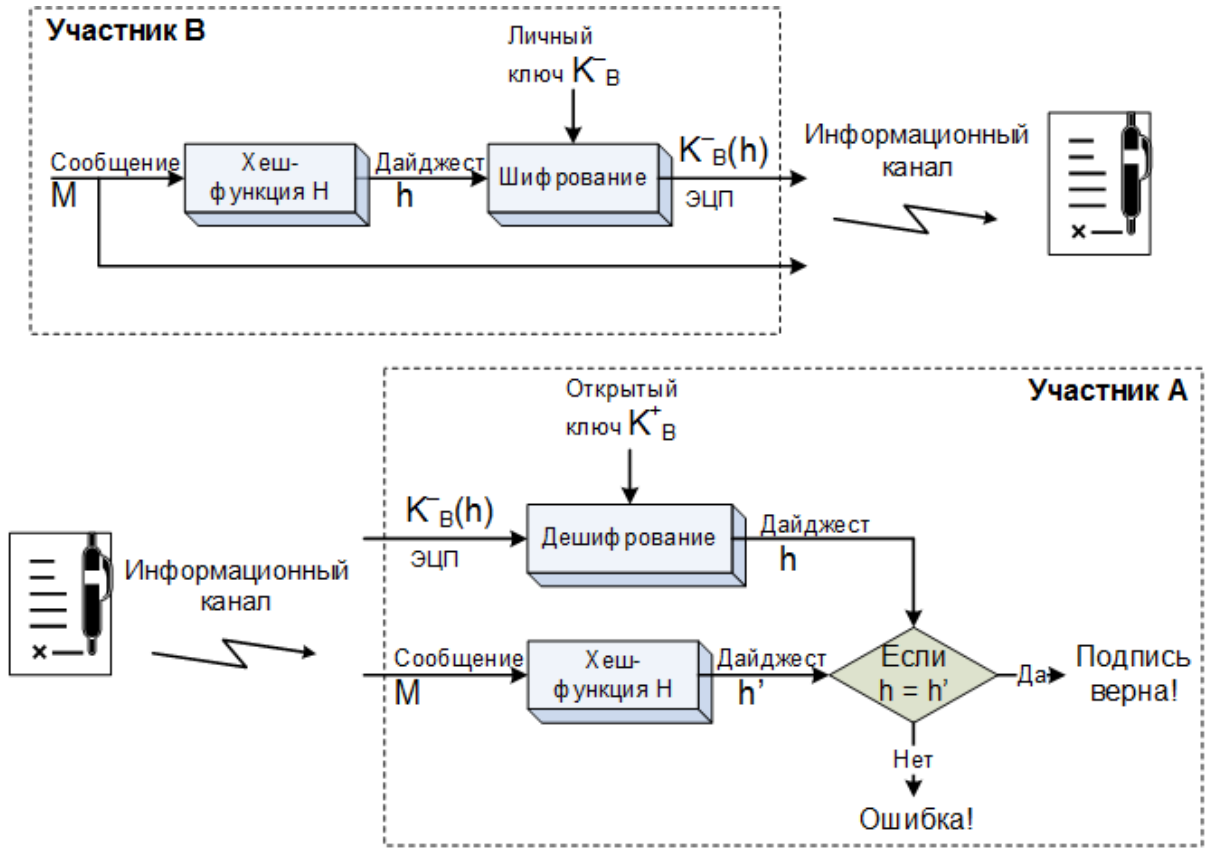


Рис. 3.13. Схема электронной подписи документа

Рассмотрим порядок действий:

1. Боб вычисляет значение дайджеста документа.

2. Боб шифрует этот дайджест своим личным ключом, таким образом

подписывая документ.

3. Боб отправляет Алисе документ и электронную цифровую подпись (зашифрованное значение дайджеста).

4. Алиса вычисляет дайджест документа, присланного Бобом.

5. Далее расшифровывает подписанное значение дайджеста с помощью открытого ключа Боба. Если подписанное значение дайджеста совпадает с рассчитанным, то цифровая подпись верна и сообщение не было подвергнуто никаким изменениям (рис. 3.13).

Чтобы избежать атаки повторного использования в цифровую подпись дополнительно включают метку времени – дату и время подписания документа.

3.5. Вредоносное программное обеспечение

Многочисленная группа атак связана с внедрением в компьютеры вредоносных программ.

Вредоносная программа (англ. malware, сокращение от malicious software – вредоносное программное обеспечение) – компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ее ресурсов, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы. В Российской Федерации создание, использование и распространение вредоносных программ наказываются, согласно Уголовному кодексу, лишением свободы.

К вредоносным программам относятся компьютерные вирусы, троянские и шпионские программы, сетевые черви, спам. На практике злоумышленники часто сочетают в одной и той же вредоносной программе их различные типы. Вредоносные программы могут проникать на атакуемые компьютеры разными способами. Самый простой из них, когда пользователь за-

гружает файлы из непроверенных источников (съемных носителей или веб-сайтов), или, не подумав, открывает подозрительный файл в письме электронной почты.

Для профилактики и диагностики проникновения вредоносных программ в вычислительную систему, а также для восстановления ее работоспособности в случае причинения ими вреда, используются ***антивирусные программы***. Антивирусы применяют в своей работе три основные группы методов:

– анализ содержимого файлов (как исполняемых, так и файлов с данными различного типа);

– отслеживание поведения программ во время их выполнения (все подозрительные действия программы контролируются и протоколируются антивирусом);

– регламентация порядка работы с файлами и программами (например, разрешение запуска только тех программ, которые имеются в списке проверенного программного обеспечения).

Рассмотрим подробнее различные типы вредоносных программ.

Черви (сетевые черви, англ. worm) – тип вредоносных программ, способных к самостоятельному распространению своих копий по каналам локальных и глобальных сетей, а также способных к автономному преодолению систем защиты автоматизированных и компьютерных систем. Так как большинство сетевых червей передаются в виде файлов, основным механизмом их распространения являются сетевые службы, основанные на файловом обмене. Так черви могут распространяться по протоколам локальных сетей или сети Интернет, с сообщениями электронной почты, через файлообменные сети и т. п.

Главная цель деятельности червя состоит в том, чтобы передать свою копию на максимально возможное количество компьютеров. Для этого зло-

умышленник определяет перечень сетевых уязвимостей, которые он собирается использовать для проведения атак средствами разрабатываемого червя. Каждый червь состоит из двух основных компонентов: атакующего блока, который рассчитан на поражение различных уязвимостей, и блока поиска целей, который собирает информацию об узлах сети для осуществления атак.

Вирус (англ. virus) – программный фрагмент, способный создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерные сети, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения.

Вирусы бывают загрузочными, заражающими загрузочные сектора постоянных и сменных носителей; файловыми, заражающими файлы; макровирусами, написанными на языке макрокоманд и исполняемыми в среде какого-либо приложения (например, макросы в документах пакета Microsoft Office); скрипт-вирусами, исполняемыми в среде определенной командной оболочки (например, Java-скрипты).

Вирус может внедрять свои фрагменты в разные типы файлов, в их начало, конец, или кусочками по всему файлу. Код вируса может быть зашифрован, чтобы затруднить его обнаружение антивирусными программами. В отличие от червей вирусы и троянские программы не содержат в себе встроенного механизма активного распространения по сети, они способны размножаться своими силами только в пределах одного компьютера. Как правило, передача копии вируса на другой компьютер происходит с участием пользователя.

Троян (троянская программа, англ. trojan) – тип вредоносных программ, которые наносят ущерб системе, маскируясь под какие-либо полезные приложения. Такие вредоносные программы могут представляться пользовате-

лю как известные программы, с которыми он работал раньше или о которых слышал, или как новые приложения с полезными для пользователя функциями.

Троянские программы можно отнести к самому простому по реализации виду вредоносных программ. Наиболее распространены следующие виды троянов:

– клавиатурные шпионы, постоянно находящиеся в оперативной памяти и сохраняющие все данные поступающие от клавиатуры с целью последующей передачи этих данных злоумышленнику;

– похитители паролей, предназначенные для получения паролей, но не использующие слежение за клавиатурой (обычно извлекают пароли из файлов, в которых они хранятся);

– утилиты удаленного управления, обеспечивающие полный удаленный контроль над компьютером пользователя;

– анонимные SMTP-сервера и прокси-сервера, выполняющие функции почтовых или прокси-серверов и использующиеся в первом случае для рассылки спама, а во втором для заметания следов хакерами;

– модификаторы настроек браузера, меняющие стартовую страницу в браузере, страницу поиска или другие настройки, для организации несанкционированных обращений к Интернет-ресурсам;

– инсталляторы прочих вредоносных программ.

Шпионские программы (англ. spyware) – программы, которые скрытно (в большинстве случаев удаленно) устанавливаются злоумышленником на компьютеры пользователей с целью отслеживания и фиксирования всех их действий. Злоумышленник может собирать информацию о параметрах компьютера, может отслеживать введение логина и пароля пользователем во время входа в систему, посещение им веб-ресурсов, обмен по сети сообщениями и данными с другими пользователями и пр.

Спам (англ. SPAM) – это атака, выполненная путем злоупотребления возможностями электронной почты. Название образовано из Shoulder Pork And haM или SPiced hAM, что в буквальном переводе означает «прессованная ветчина с пряностями». Когда-то американская фирма-изготовитель этих консервов рассылала рекламу своего товара по обычным почтовым ящикам жителей страны.

Учитывая популярность и важную роль электронной почты в работе современных предприятий и организаций, можно сказать, что спам в последнее время является существенной угрозой безопасности. Спам отнимает время и ресурсы на просмотр и удаление бесполезных сообщений, при этом ошибочно могут быть удалены письма с критически важной информацией. Посторонняя почта, не только снижает эффективность работы предприятия, но часто служит средством внедрения вредоносных программ. По статистическим данным сайта www.senderbase.org компании Cisco на легальную электронную почту за период с ноября 2014 по ноябрь 2015 г. приходится всего 13,87 % всех электронных сообщений; 86,12 % – это спам и менее 0,01 % – другое вредоносное ПО (рис. 3.14).

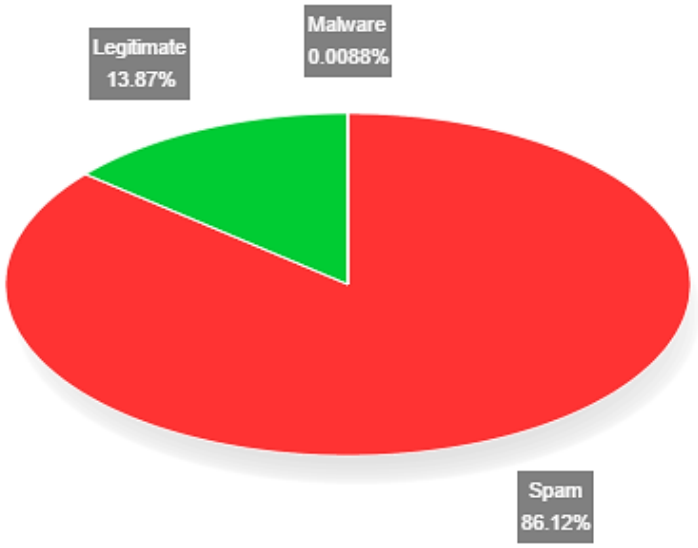


Рис. 3.14. Количество спама в электронной почте по данным сайта www.senderbase.org

КОНТРОЛЬНЫЕ ЗАДАНИЯ

Лабораторные работы

Работа № 1. Для выполнения данной работы создайте текстовый документ, в который вносите решения заданий согласно Вашему варианту.

Вариант 1

1. Восстановите исходный IP-адрес по фрагментам:

.64	2.16	16	8.132

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

ftp://ftp.ru/all_ftp/docs/New/2.doc

3. Доступ к файлу index.html, размещенному на сервере www.ftp.ru, осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

.html	www.	/	ftp	.ru	http	index	://

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.ar». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 2

1. Восстановите исходный IP-адрес по фрагментам:

3.12	21	2.12	.42

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

http://www.mathesis.ru/books/ladenburg/ladenburg.djvu

3. На сервере news.edu находится файл list.txt, доступ к которому осуществляется по протоколу ftp. Восстановите URL-адрес этого файла по при-

веденным фрагментам.

.html	www.	/	ftp	.ru	http	index	://

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.bg». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 3

1. Восстановите исходный IP-адрес по фрагментам:

.64	3.13	3.133	20

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

https://www1.ege.edu.ru/schedule/index.html

3. На сервере school.edu находится файл rating.net, доступ к которому осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

edu	school	.net	/	rating	http	://

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.cl». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 4

1. Восстановите исходный IP-адрес по фрагментам:

2.19	.50	5.162	22

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

http://www.radio.ru/p2010.png

3. На сервере info.edu находится файл exam.net, доступ к которому осу-

ществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

info	/	.net	.edu	http	exam	://

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.de». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 5

1. Восстановите исходный IP-адрес по фрагментам:

3.133	22	.73	4.13

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

ftp://ftp.intel.com/IntelUserGuides.htm

3. На сервере test.edu находится файл demo.net, доступ к которому осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

test	demo	://	/	http	.edu	.net

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.fi». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 6

1. Восстановите исходный IP-адрес по фрагментам:

.28.	24	9.9	28

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

ftp://ftp.radio.ru/pub/2015/11/12.pdf

3. На сервере info.edu находится файл list.doc, доступ к которому осуществляется по протоколу ftp. Восстановите URL-адрес этого файла по приведенным фрагментам.

info	list	://	.doc	ftp	.edu	/

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.il». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 7

1. Восстановите исходный IP-адрес по фрагментам:

3.231	3.25	.64	18

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

http://iite.unesco.org/pics/publications/ru/files/3214728.pdf

3. Доступ к файлу http.txt, находящемуся на сервере www.net, осуществляется по протоколу ftp. Восстановите URL-адрес этого файла по приведенным фрагментам.

://	http	ftp	.net	.txt	/	www

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.at». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 8

1. Восстановите исходный IP-адрес по фрагментам:

.175.5	51.	152	8

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

ftp://ftp.radio.ru/pub/Melody/Melody.rar

3. Доступ к файлу ftp.net, находящемуся на сервере txt.org, осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

.net	ftp	://	http	/	.org	txt

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.br». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 9

1. Восстановите исходный IP-адрес по фрагментам:

2.222	.32	22	2.22

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

http://www.qgistutorials.com/ru/docs/making_a_map.html

3. Доступ к файлу htm.net, находящемуся на сервере com.edu, осуществляется по протоколу ftp. Восстановите URL-адрес этого файла по приведенным фрагментам.

/	com	.edu	://	.net	htm	ftp

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.cn». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 10

1. Восстановите исходный IP-адрес по фрагментам:

.42	6.242	2.22	20

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

ftp://ftp.intel.com/images/UserTroubleshootingPic2.JPG

3. Доступ к файлу info.doc, находящемуся на сервере ege.ru, осуществляется по протоколу ftp. Восстановите URL-адрес этого файла по приведенным фрагментам.

/	ege.	info	ftp	.doc	://	ru

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.dk». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 11

1. Восстановите исходный IP-адрес по фрагментам:

5.162	22	.50	2.19

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

www.microsoft.com/ru-ru/softmicrosoft/Project2013pro.aspx

3. На сервере info.edu находится файл exam.net, доступ к которому осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

.edu	/	.net	info	http	exam	://

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.gr». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 12

1. Восстановите исходный IP-адрес по фрагментам:

2.12	21	3.31	.42

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

ftp://ftp.mccme.ru/pub/video/2008-06-10-vesti.avi

3. На сервере info.edu находится файл exam.net, доступ к которому осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

index	.ru	/	ftp	www.	http	.html	://

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.is». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 13

1. Восстановите исходный IP-адрес по фрагментам:

9.8	24	.28.	28

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

http://book.kbsu.ru/theory/chapter4/1_4_13.html

3. На сервере info.edu находится файл exam.net, доступ к которому осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

.edu	list	://	info	ftp	.doc	/

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.kg». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 14

1. Восстановите исходный IP-адрес по фрагментам:

.50	2.19	5.162	22

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

ftp://ftp.redcom.ru/pub/Java/jicra-1.2.1.zip

3. На сервере info.edu находится файл exam.net, доступ к которому осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

test	demo	://	/	http	.edu	.net

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.li». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

Вариант 15

1. Восстановите исходный IP-адрес по фрагментам:

8.132	2.16	16	.64

2. В приведенном URL-адресе выпишите протокол доступа, доменное имя сервера, путь к файлу, имя файла:

http://kvant.mccme.ru/1992/04/algoritm.htm

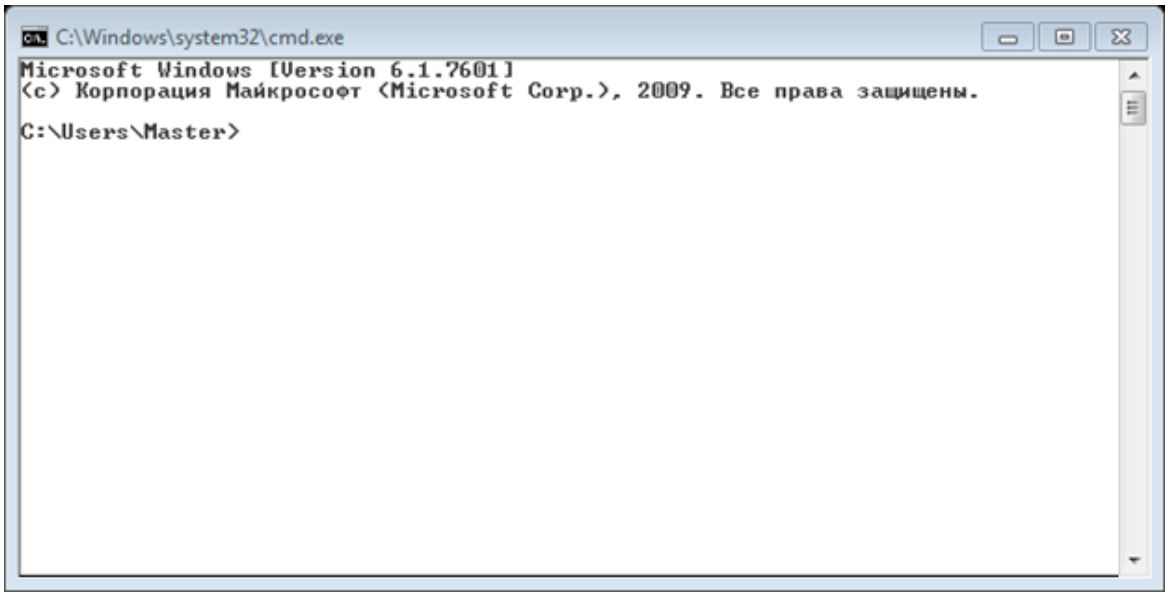
3. На сервере info.edu находится файл exam.net, доступ к которому осуществляется по протоколу http. Восстановите URL-адрес этого файла по приведенным фрагментам.

ftp	www.	/	.html	.ru	http	index	://

4. С помощью поисковой системы Google или Yandex определите, какой стране принадлежит географический домен верхнего уровня «.my». Используя оператор поисковых запросов «site:» в Google или «domain:» в Yandex, найдите и запишите в отчет URL-адреса трех любых сайтов в данном домене.

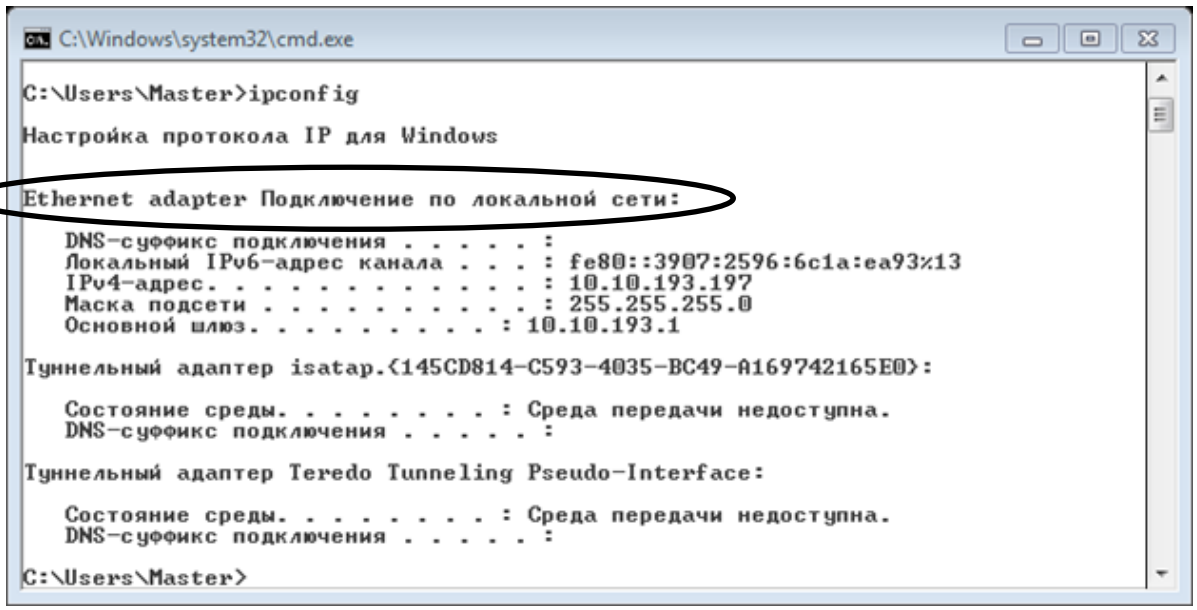
Работа № 2. В данной работе познакомимся с тремя командами операционной системы Microsoft Windows – ipconfig, ping и getmac, использующимися при работе с компьютерной сетью.

Для выполнения системных команд в операционной системе Windows имеется утилита cmd.exe, которая открывает окно с командной строкой. Для ее запуска необходимо зайти в главное меню Пуск → Все программы → Стандартные → Командная строка.



В окне командной строки отображается полный путь к текущей рабочей папке (на рис. это «C:\Users\Master») и закрывающая угловая скобка > (символ «больше») в конце, указывающая, что после нее может вводиться команда. Чтобы просмотреть список часто используемых команд, введите в командной строке help и нажмите клавишу Enter.

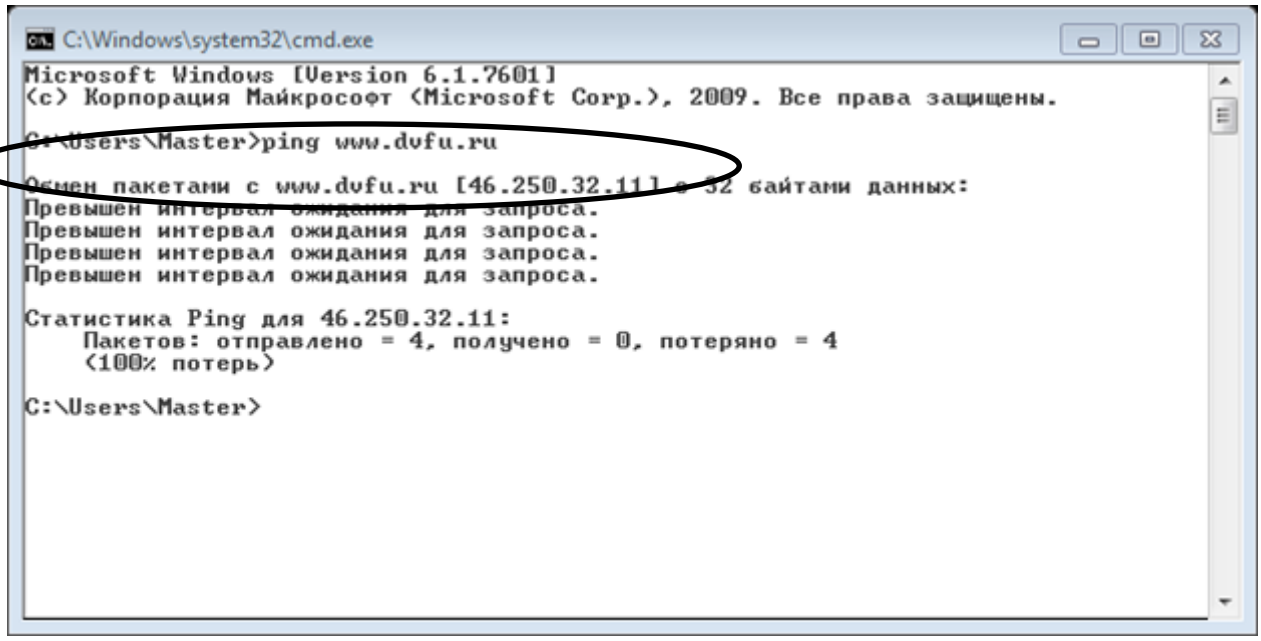
Команда ipconfig выводит детали текущего соединения компьютера в сети и управляет некоторыми сетевыми сервисами. Для вывода сведений команда используется без параметров. Например, нас интересует IP-адрес своего рабочего компьютера в локальной сети. Вводим в командную строку ipconfig. В полученном результате находим адаптер с именем сетевого подключения и строку IPv4 с цифровым адресом.



Команда ping используется для проверки соединений в сетях. Будем использовать команду в двух вариантах:

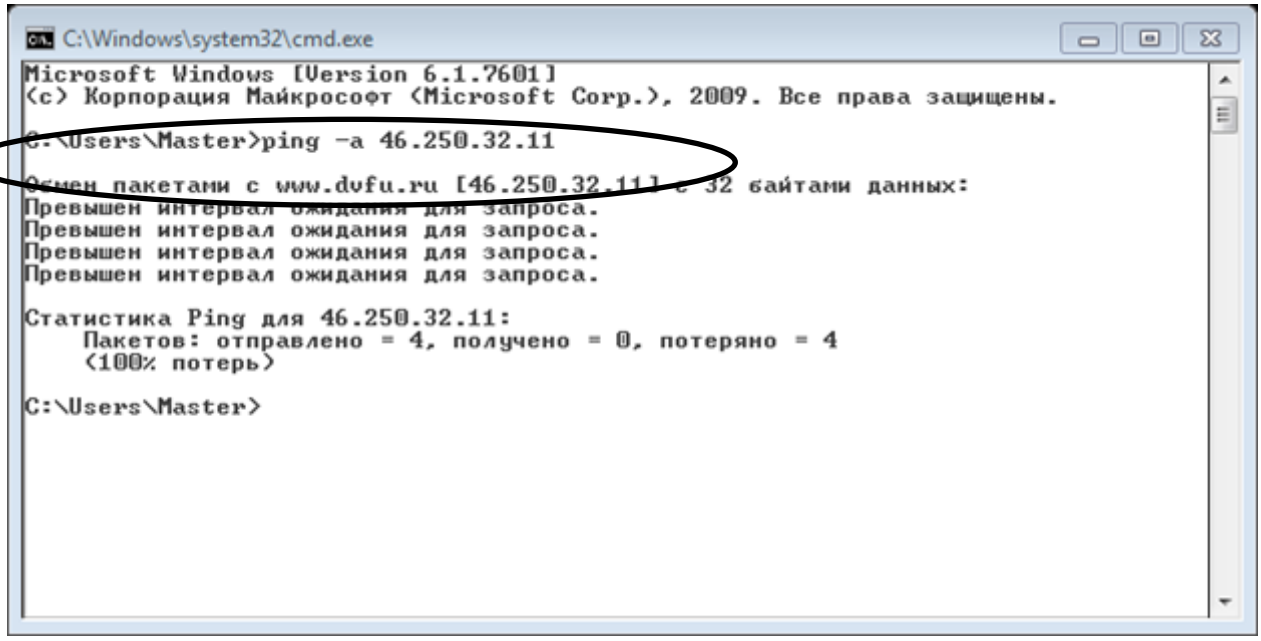
`ping` конечный_узел и `ping -a` конечный_узел

В обоих случаях эта команда отправляет запросы на имя или IP-адрес узла сети и ожидает ответные сообщения, подтверждающие, что связь имеется. Например, в командную строку была введена команда ping с доменным адресом веб-сервера www.dvfu.ru и получен результат.



В результате указан IP-адрес, соответствующий доменному адресу узла, время ответа на отправленные запросы, приблизительное время приема-передачи запросов.

Второй вариант с параметром `-a` можно использовать для определения доменного имени узла по IP-адресу (рис. 3.18).



Команда getmac предназначена для отображения MAC-адресов сетевых адаптеров локального или удаленного компьютера. Для отображения подробной информации с указанием подключения и названия сетевого адаптера команда используется с параметром /v: «getmac /v».

Задание 1

Для выполнения данной работы создайте текстовый документ. В документ добавьте таблицу и заполните ее полученными результатами заданий 1, 2 и 3.

Пример оформления решения заданий 1, 2 и 3

Компьютер/доменный адрес	IP-адрес	Класс IP-адреса
Рабочий компьютер	10.10.193.197	A
www.dvfu.ru	46.250.32.11	A
pnu.edu.ru	…	…
…	…	…

Используя команду ipconfig определите IP-адрес Вашего рабочего компьютера в локальной сети. Запишите класс полученного адреса.

Задание 2

Используя команду ping, определите цифровой IP-адрес:

– веб-сервера по доменному адресу согласно варианту табл. 6;

– веб-сервера официального сайта Тихоокеанского государственного университета по доменному адресу pnu.edu.ru.

Варианты задания 2

Вариант	Доменный адрес
1.	mail.ru
2.	yandex.ru
3.	google.ru
4.	rambler.ru
5.	yahoo.com
6.	vk.com
7.	odnoklassniki.ru
8.	facebook.com
9.	twitter.com
10.	sberbank.ru
11.	pochta.ru
12.	rosneft.ru
13.	instagram.com
14.	gazprom.ru
15.	microsoft.com

Задание 3

Используя команду ping с параметром -a, определите доменные имена по следующим IP-адресам:

– 94.100.180.26;

– 81.19.70.3;

– 217.151.130.37.

Задание 4

Используя команду getmac с параметром /v, определите и внесите в документ название сетевого адаптера и его MAC-адрес.

Задание 5

1. Откройте веб-браузер. В адресную строку вместо доменного имени веб-сервера введите IP-адрес, полученный Вами в задании 2, и перейдите по нему. Убедитесь, что при вводе IP-адреса в адресную строку браузера, он переходит на соответствующий веб-сайт.

2. Откройте Проводник Windows. В строке адреса введите IP-адрес файлового сервера Тихоокеанского государственного университета \\10.10.10.10. Просмотрите его содержимое.

Сетевые папки сервера позволяют пользователям обмениваться информацией, а также хранить свои файлы в этих папках с разными правами доступа:

– в открытом доступе с возможностью изменения (обычно папка называется «Incoming»);

– в открытом доступе без возможности изменения другими пользователями, кроме владельца (обычно папка называется «Shared»);

– в закрытом доступе (доступ к папке предоставляется отдельным пользователям).

Задание 6

Откройте веб-браузер. В адресной строке перейдите через протокол ftp к любому из предложенных FTP-серверов:

– ftp.intel.com (FTP-сервер компании Intel);

– ftp.mccme.ru (FTP-сервер Московского центра непрерывного математического образования);

– ftp.redcom.ru (FTP-сервер компании Redcom);

– ftp.radio.ru (FTP-сервер журнала «Радио»).

Ознакомьтесь со структурой папок сервера. Скопируйте с сервера в свою рабочую папку 3 любых файла. Для этого на имени выбранного файла

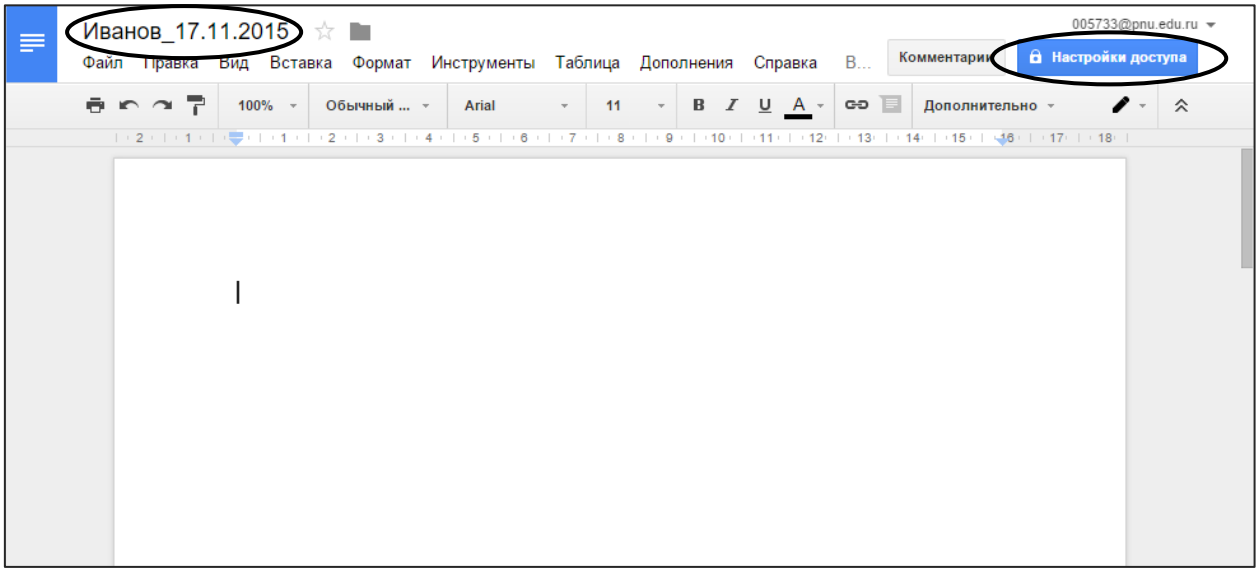
нажмите правую кнопку мыши и в появившемся контекстном меню выберите команду «Сохранить ссылку как…».

Работа № 3. В данной работе освоим использование некоторых облачных приложений Google Apps. Для этого потребуется данные учетной записи Google. Выберите себе в группе напарника и обменяйтесь с ним адресами электронной почты в домене @pnu.edu.ru или @gmail.com.

Задание 1. Google Документы

1. Откройте текстовый редактор Google Документы (docs.google.com) и создайте в нем новый документ. Назовите его по Вашей фамилии и текущей дате (например, Иванов_17.11.2015).

2. С помощью кнопки «Настройки доступа» предоставьте доступ к этому документу Вашему напарнику с правом редактирования и преподавателю с правом чтения.



3. После того, как напарник предоставит Вам доступ к своему документу, дополните его произвольным текстом или внесите следующий текст: «В настоящее время сложилось три модели использования сервисов облачных вычислений: инфраструктура как сервис (IaaS), платформа как сервис (PaaS), приложение как сервис (SaaS)».

4. Обратите внимание, что после внесения изменений в документе показано, кто их внес.

5. Убедитесь, что теперь у Вас в облачном хранилище имеются два документа – Ваш и напарника.

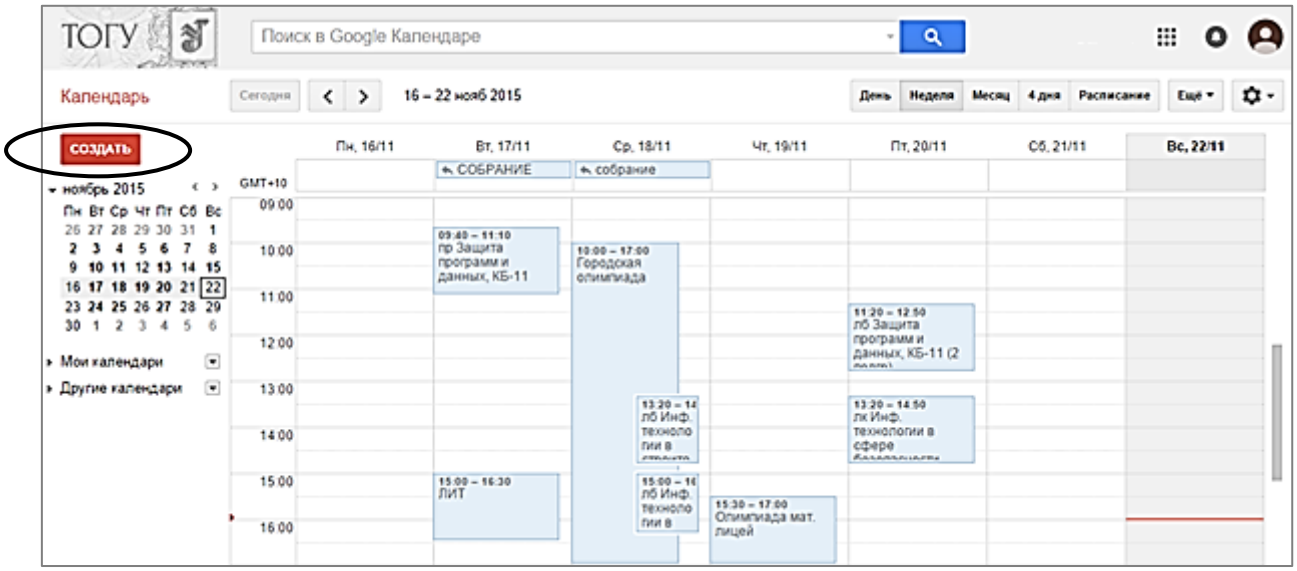
Задание 2. Google Календарь

1. Откройте приложение Google Календарь (calendar.google.com) и создайте в нем следующие мероприятия:

– единоразовое (например, собрание);

– на весь день (например, день рождения одногруппника);

– повторяющееся (например, первая пара каждый понедельник).



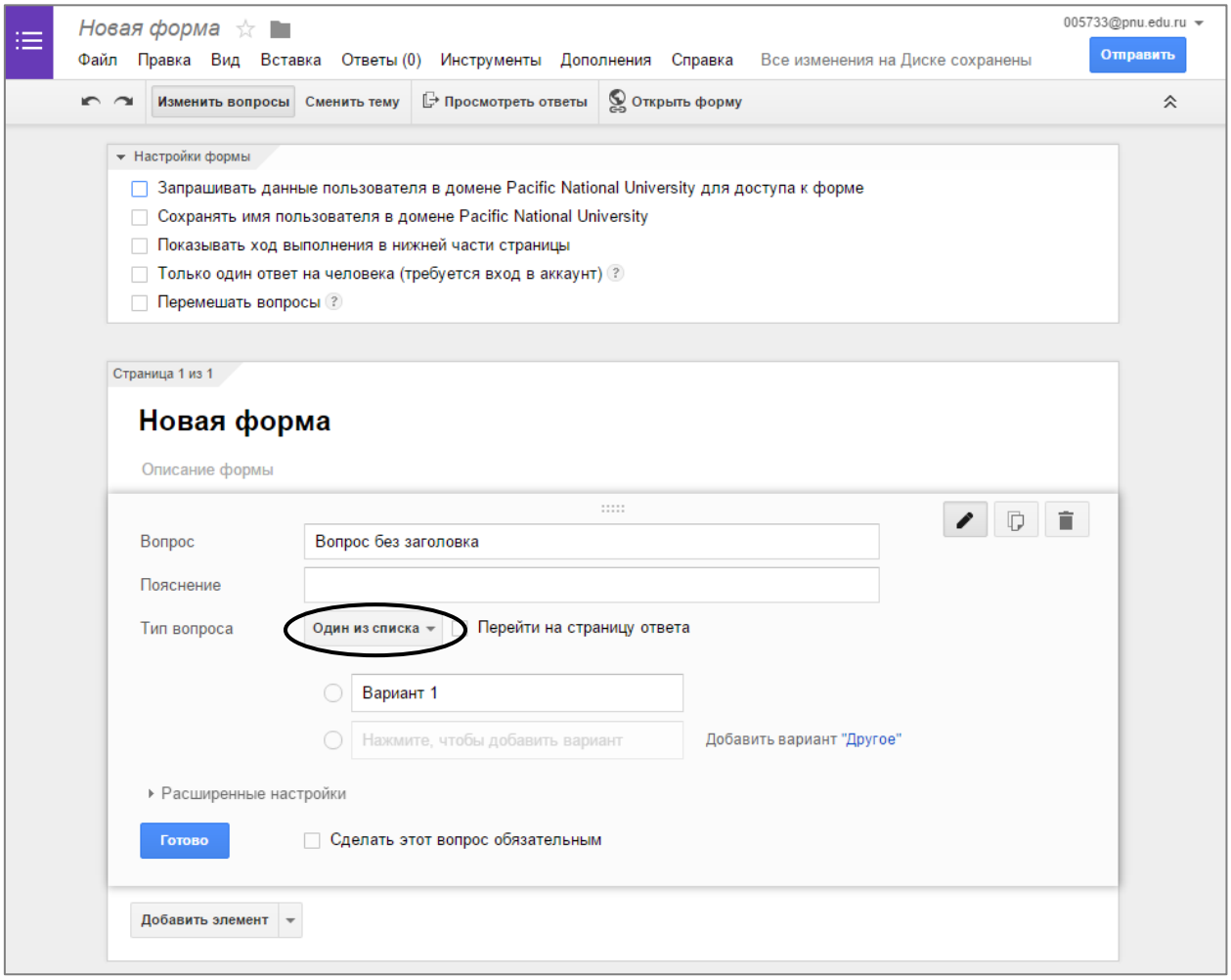
Для всех мероприятий укажите даты и время, места проведения, Ваш статус на время мероприятия (доступен или занят). Для единоразового мероприятия настройте оповещение по электронной почте и пригласите напарника и преподавателя в качестве гостей мероприятия.

2. Создайте отдельный календарь для общественных мероприятий, в которых Вы принимаете участие. Откройте общий доступ к этому календарю всем пользователям. Добавьте в этот календарь 2-3 произвольных события на текущей неделе.

3. В настройках созданного календаря скопируйте html-адрес календаря и отправьте его напарнику и преподавателю по электронной почте.

Задание 3. Google Формы

1. Откройте приложение Google Формы (docs.google.com/forms) и создайте в нем анкету или опросник по любой тематике. Предусмотрите наличие вопросов разного типа: с выбором одного ответа из списка, с выбором нескольких ответов из списка, с полем для ввода краткого ответа и т. д.



2. Отправьте по электронной почте напарнику URL-адрес формы. Заполните друг другу несколько анкет.

3. Просмотрите сводный отчет ответов с диаграммами по проведенному анкетированию.

4. Откройте преподавателю доступ к форме с анкетой, табличному файлу с результатами опроса и сводными диаграммами.

Тесты

Укажите правильный ответ.

1. Если адрес сервера www.academia.edu.ru, то именем домена верхнего уровня в нем является

а) ru;

б) www;

в) edu;

г) edu.ru.

2. Аппаратное обеспечение локальной вычислительной сети включает

а) рабочие станции, сервер, коммуникационное оборудование;

б) рабочие станции, коммуникационное оборудование, персональные компьютеры;

в) коммуникационное оборудование, сервер;

г) компьютеры, подключенные к сети и обеспечивающие пользователей определенными услугами.

3. Персональный компьютер, подключенный к сети и обеспечивающий доступ пользователя к ее ресурсам, называется

а) рабочей станцией;

б) сервером;

в) хостом;

г) доменом.

4. Сетевым протоколом является

а) PPP;

б) WWW;

в) ECP;

г) URL.

5. Устройство, обеспечивающее соединение административно независимых коммуникационных сетей, называется

а) роутером;

б) хостом;

в) доменом;

г) концентратором.

6. Сетевые операционные системы – это комплекс программ, которые

а) обеспечивают одновременную работу группы пользователей;

б) пользователи переносят в сети с одного компьютера на другой;

в) обеспечивают обработку, передачу и хранение данных на компьютере;

г) расширяют возможности многозадачных операционных систем.

7. Если адрес электронной почты в сети Интернет pochta@mail.ru, то именем почтового сервиса в нем является

а) mail;

б) pochta;

в) mail.ru;

г) ru.

8. Шлюз – это устройство, которое

а) позволяет организовать обмен данными между двумя сетями, использующими различные протоколы взаимодействия;

б) позволяет организовать обмен данными между двумя сетями, использующими один и тот же протокол взаимодействия;

в) соединяет сети разного типа, но использующие одну операционную систему;

г) соединяет рабочие станции.

9. Поставщиком Интернет-услуг является

а) провайдер;

б) компьютер, подключенный к Интернету;

в) браузер;

г) модем, подключенный к сети Интернет.

10. На сервере graphics.sc находится файл picture.gif, доступ к которому осуществляется по протоколу ftp. Правильно записанным адресом указанного файла является

а) ftp://graphics.sc/picture.gif;

б) ftp://picture.gif/graphics.sc;

в) ftp://graphics.sc.picture.gif;

г) ftp://picture.gif.graphics.sc.

11. В соответствии со стандартом скорость передачи информации по сети может измеряться в

а) кбит/с;

б) кбайт/мин;

в) кбит/мин;

г) кбайт/с.

12. Документ запрашивается со страницы сайта университета по следующему адресу: http://university.faculty.edu/document.txt. Доменным именем компьютера, в котором находится документ, является

а) university.faculty.edu;

б) university;

в) faculty;

г) university.faculty.

13. Для быстрого перехода от одного www-документа к другому используется

а) гиперссылка;

б) браузер;

в) сайт;

г) тег.

14. Компьютер, подключенный к Интернету, обязательно должен

а) получить IP-адрес;

б) иметь установленный web-сервер;

в) получить доменное имя;

г) иметь размещенный на нем web-сайт.

15. Для просмотра web-страниц используются

а) браузеры;

б) Интернет-порталы;

в) Брандмауэры;

г) программы хэширования.

16. Как известно, IP-адрес компьютера состоит из четырех чисел, разделенных точками. Каждое из чисел IP-адреса может принимать десятичные значения от 0 до

а) 255;

б) 256;

в) 999;

г) 192.

17. Топологиями локальных вычислительных сетей являются

а) звезда, шина, кольцо;

б) ромашка, сфера, звезда;

в) серверная, доменная, терминальная;

г) корпоративная, административная, смешанная.

18. Компьютер, подключенный к сети Интернет, может иметь два следующих адреса:

а) цифровой и доменный;

б) цифровой и пользовательский;

в) символьный и доменный;

г) прямой и обратный.

19. Система обмена через Интернет мгновенными сообщениями называется

а) ICQ;

б) IRC;

в) URL;

г) GPS.

20. Сетевой сервис FTP предназначен для

а) перемещения данных между различными операционными системами;

б) проведения видеоконференций;

в) просмотра web-страниц;

г) «скачивания» сообщений и приложенных файлов.

21. Мост – это устройство, соединяющее

а) две сети, использующие одинаковые методы передачи данных;

б) две сети, имеющие одинаковый сервер;

в) рабочие станции одной сети;

г) абонентов локальной вычислительной сети.

22. Для поиска информации в сети Интернет с помощью поисковых систем (например, Google, Rambler, Yandex, Yahoo!) пользователи задают

а) ключевые слова;

б) теги;

в) поисковые слова;

г) словарные слова.

23. Если адрес электронной почты в сети Интернет postbox@yandex.ru, то именем владельца этого электронного адреса является

а) postbox;

б) yandex;

в) yandex.ru;

г) postbox@.

24. Вредоносная программа, проникающая в компьютер под видом другой программы (известной и безвредной) и имеющая при этом скрытые деструктивные функции, называется

а) «троянский конь»;

б) «компьютерный червь»;

в) стэлс-вирус;

г) макровирус.

25. Чтобы наладить обмен электронными сообщениями, имеющими цифровую подпись, необходимо передать получателю сообщений

а) открытый ключ шифрования;

б) закрытый ключ шифрования;

в) вид вашей цифровой подписи;

г) используемый вами алгоритм шифрования.

26. Для подключения компьютера к локальной сети необходимы

а) модем и сетевая карта;

б) сетевая карта и витая пара;

в) модем и коммутируемая линия связи;

г) модем, сетевая карта и коммутируемая линия связи.

27. Клиент – это

а) компьютер, используемый абонентом для получения и передачи информации;

б) компьютер, обеспечивающий информационные услуги в сети;

в) программа, подготавливающая запрос пользователя, передающая этот запрос по сети, а затем принимающая ответ.

28. Протоколы POP3 и SMTP используются для организации сервиса

а) облачные вычисления;

б) обмен мгновенными сообщениями;

в) электронная почта;

г) WWW.

29. Модель OSI (Open System Interconnection) является

а) объединением национальных организаций по стандартизации;

б) международной программой по стандартизации обмена данными между сетевыми устройствами;

в) межсетевым протоколом, на котором основана сеть Интернет;

г) системой адресации компьютеров в сети.

30. Необходимо послать электронное сообщение удаленному адресату. При этом получатель должен знать, что это именно то самое сообщение. Для этого нужно

а) использовать цифровую подпись;

б) послать сообщение по секретному каналу связи;

в) заархивировать сообщение;

г) закрыть сообщение паролем.

31. Вирус, внедряющийся в исполняемые файлы и активизирующийся при их запуске, называется

а) загрузочным;

б) макровирусом;

в) файловым;

г) «сетевым червем».

32. Сетевым протоколом является

а) MAC;

б) WWW;

в) IP;

г) URL.

33. Для хранения файлов, предназначенных для общего доступа пользователям локальной сети организации, используется

а) хост-компьютер;

б) файл-сервер;

в) клиент-сервер;

г) сервер базы данных.

34. Осуществляют ли публичные сервисы электронной почты (такие как mail.ru, gmail.com и т. п.) проверку электронных писем на наличие вирусов?

а) Да, но только на наличие угроз серверам почтовой системы.

б) Да, все письма проверяются, и сомнительные удаляются или помечаются специальным знаком.

в) Нет, почта не проверяется.

г) Зависит от настроек пользователя.

ЗАКЛЮЧЕНИЕ

Тема «Компьютерные сети» очень широка и многогранна, а быстрый рост числа компьютерных сетей и их развитие сопровождаются сменой или совершенствованием сетевых технологий. Изучая информатику, важно понимать базовые основы и принципы построения и функционирования компьютерных сетей без углубления в детали. Именно с этой точки зрения мы и постарались изложить материал в данном учебном пособии. Читатели, заинтересовавшиеся более подробным изучением рассмотренной темы, могут воспользоваться рекомендованными дополнительными источниками из приведенного далее списка.

РЕКОМЕНДАТЕЛЬНЫЙ БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Акулов, О. А.* Информатика: базовый курс : учеб. пособие для студ. вузов / О. А. Акулов, Н. В. Медведев. – М. : Омега-Л, 2005. – 552 с.

2. *Ватаманюк, А.* Создание, обслуживание и администрирование сетей на 100 % / А. Ватаманюк. – СПб. : Питер, 2010. – 288 с.

3. *Вирусы* и средства борьбы с ними // НОУ «ИНТУИТ». – Режим доступа: http://www.intuit.ru/studies/courses/1042/154/info (дата обращения: 01.02.2016).

4. *ГОСТ 28147–89.* Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования // Национальные стандарты. – Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=139177 (дата обращения: 01.02.2016).

5. *Дергачева, Л. М.* Решение типовых экзаменационных задач по информатике: учеб. пособие / Л. М. Дергачева. – М. : БИНОМ. Лаборатория знаний, 2013. – 360 с.

6. *Зиангирова, Л.* Технологии облачных вычислений // НОУ «ИНТУИТ». – Режим доступа: http://www.intuit.ru/studies/courses/3508/750/lecture/27409 (дата обращения: 01.02.2016).

7. *Информационно-коммуникационные* технологии. Цифры и факты // Международный союз электросвязи. – Режим доступа: http://www.itu.int/en/

ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (дата обращения: 01.02.2016).

8. *Колисниченко, Д. Н.* Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание / Д. Н. Колисниченко. – СПб. : Наука и техника, 2004. – 400 с.

9. *Куроуз, Дж.* Компьютерные сети / Дж. Куроуз, К. Росс. – СПб. : Питер, 2004. – 765 с.

10. *Лапонина, О. Р.* Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учеб. пособие / О. Р. Лапонина. – М.: Интернет-Ун-т Информ. Технологий, 2005. – 608 с.

11. *Малясова, С. В.* Информатика и ИКТ : пособие для подготовки к ЕГЭ / С. В. Малясова, С. В. Демьяненко. – М. : Академия, 2014. – 304 с.

12. *Материалы* свободной энциклопедии Википедия // Википедия. Режим доступа: http://ru.wikipedia.org/ (дата обращения: 01.02.2016).

13. *Об электронной* цифровой подписи : федеральный закон от 10.01.2002 № 1 // Справочно-правовая система «Консультант Плюс» / Компания «Консультант Плюс».

14. *Олифер, В. Г.* Компьютерные сети. Принципы, технологии, протоколы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2013. – 944 с.

15. *Олифер, В. Г.* Основы компьютерных сетей: учеб. пособие / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2014. – 352 с.

16. *Олифер, В. Г.* Сетевые операционные системы / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2002. – 544 с.

17. *Основы* компьютерных сетей : учеб. пособие. Корпорация Microsoft. – М. : БИНОМ. Лаборатория знаний, 2006. – 167 с.

18. *Риз, Д.* Облачные вычисления (Cloud Application Architectures) / Д. Риз. – СПб. : БХВ-Петербург, 2011. – 288 с.

19. Сведения об МСЭ // Международный союз электросвязи [Электронный ресурс]. – Режим доступа: http://www.itu.int/ru/about/Pages/default.aspx

20. *Соснин, В.* Облачные вычисления в образовании // НОУ «ИНТУИТ». – Режим доступа: http://www.intuit.ru/studies/courses/12160/1166/info (дата обращения: 01.02.2016).

21. *Шнайер, Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

ПРИЛОЖЕНИЕ

Некоторые полезные ресурсы сети Интернет

Содержимое	Адрес
Карта сети Интернет	http://www.opte.org/the-internet/ http://internet-map.net/ http://www.peer1.com/map-of-the-internet-infographic
Карта подводного кабеля	http://www.submarinecablemap.com/
О том, как устроены трансокеанические подводные кабели связи	http://habrahabr.ru/post/228415/
Интернетометр Яндекс (IP-адрес, скорость Интернет-соединения и другая техническая информация о вашем компьютере)	http://yandex.ru/internet
Информация о вашем IP-адресе	http://www.whatismyip.com/
Интерактивная карта киберугроз от Лаборатории Касперского	https://cybermap.kaspersky.com/
Изображение в реальном времени мировых кибератак	http://map.norsecorp.com/
Карта мониторинга электронной почты и веб-трафика	http://www.senderbase.org/
Виртуальный компьютерный музей (имеется раздел «История развития электросвязи»)	http://www.computer-museum.ru/
Хабаровский компьютерный музей	http://xkm.su/
Яндекс-Каталог	http://yaca.yandex.ru/
Каталог Mail.ru	http://list.mail.ru/11028/1/0_1_0_1.html

Учебное издание

Стригунов Валерий Витальевич

ВВЕДЕНИЕ В КОМПЬЮТЕРНЫЕ СЕТИ

Учебное пособие

Дизайнер обложки *Е. Саморядова*

С авторского оригинала-макета

Подписано в печать 08.02.16. Формат 60 x 84 $^{1}/_{16}$. Бумага писчая. Гарнитура «Калибри».
Печать цифровая. Усл. печ. л. 6,10. Тираж 100 экз. Заказ 22.

Издательство Тихоокеанского государственного университета.
680035, Хабаровск, ул. Тихоокеанская, 136.

Отдел оперативной полиграфии издательства Тихоокеанского государственного университета.
680035, Хабаровск, ул. Тихоокеанская, 136.