Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
"САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ"

С.А. Чеверева

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие
для студентов вузов

Самара
Издательство
Самарского государственного экономического университета
2018

УДК 331.54:004
ББК 3973.2я7
Ч-34

Рецензенты: кандидат технических наук, доцент ФГБОУ ВО "ПГУТИ" Н.В. Киреева;
кандидат педагогических наук, доцент О.И. Пугач

Издается по решению
редакционно-издательского совета университета

Чеверева, Светлана Александровна.

Ч-34 Информационно-коммуникационные технологии в профессиональной деятельности [Электронный ресурс] : учеб. пособие для студентов вузов / С.А. Чеверева. - Самара : Изд-во Самар. гос. экон. ун-та, 2018. - 1 электрон. опт. диск. - Систем. требования: процессор Intel с тактовой частотой 1,3 ГГц и выше ; 256 Мб ОЗУ и более ; MS Windows XP/Vista/7/10 ; Adobe Reader ; разрешение экрана 1024×768 ; привод CD-ROM. - Загл. с титул. экрана. - № гос. регистрации: 0321901128.

ISBN 978-5-94622-890-9

В учебном пособии рассмотрены классификация и архитектура вычислительных сетей, техническое, информационное и программное обеспечение, структура и организация функционирования сетей, облачные и мобильные технологии, электронные сервисы. Представлены структура и характеристики систем телекоммуникаций, базовые технологии, описана сетевая модель и протоколы стека TCP/IP, настройка подключения к сети, а также основные сервисы сети Internet. Даны понятия сетевой безопасности и направления ее обеспечения. Рассматриваются вопросы глобализации, облачные сервисы, хранение данных, требования и методы защиты информации в корпоративных системах.

Предназначено для студентов всех направлений, изучающих дисциплину "Информационно-коммуникационные технологии в профессиональной деятельности". Может быть рекомендовано студентам и преподавателям других направлений любой формы обучения при изучении и практическом конфигурировании компьютерных сетей.

УДК 331.54:004
ББК 3973.2я7

ISBN 978-5-94622-890-9

Оглавление

Введение

Процессы информатизации в современном обществе, а также тесно связанная с ними реформа образовательной деятельности характеризуются совершенствованием и массовым распространением современных информационно-коммуникационных технологий (ИКТ). Их активно используют для передачи данных и обеспечения взаимодействия учителя и обучаемого в современной системе дистанционного и открытого образования. Сегодня преподаватель обязан не только владеть навыками в сфере ИКТ, но и отвечать за профессиональное применение информационно-коммуникационных технологий в своей непосредственной деятельности. Термин "технология" пришел к нам из греческого языка, в переводе он означает "наука". Современное понимание данного слова включает в себя применение инженерных и научных знаний для решения конкретных практических задач. Тогда информационно-коммуникационная технология - это такая технология, которая направлена на преобразование и обработку информации. Но и это еще не все. По сути, информационно-коммуникационная технология является обобщающим понятием, описывающим различные механизмы, устройства, алгоритмы, способы обработки данных.

Важнейшим современным устройством ИКТ выступает компьютер, снабженный необходимым программным обеспечением. Не менее значимыми считаются средства коммуникации с размещенной на них информацией. Компьютерные сети - это целый мир интереснейших событий, сведений и технологий, над основными из которых ведется работа уже несколько десятилетий.

1. КЛАССИФИКАЦИЯ, НАЗНАЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

1.1. Основные понятия сетей. Классификация сетей

Сеть (граф, net) - это множество произвольных элементов (узлов, вершин), связанных между собой линиями связи (ребрами, дугами).

Сети могут быть как материальными, так и абстрактными (рис. 1).

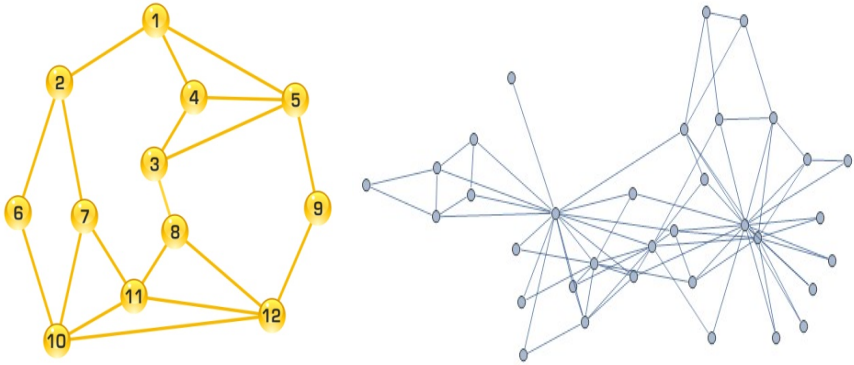

Рис. 1. **Сети**

Информационная сеть (вычислительная, компьютерная, коммуникационная сеть, network, КС) - это система распределенных на территории аппаратных, программных и информационных ресурсов, связанных между собой каналами передачи данных. Самая известная и обширная компьютерная сеть - Internet.

Вычислительная сеть - это совокупность компьютеров и другого периферийного оборудования, соединенных с помощью каналов связи в единую систему так, что они могут связываться между собой и совместно использовать ресурсы сети.

В зависимости от того, какие абоненты входят в сеть, они называются:

- одноранговые сети;
- сети с выделенным сервером.

По составу вычислительных средств они подразделяются:

- на однородные - объединяют однородные вычислительные средства (компьютеры);
- неоднородные - объединяют различные вычислительные средства (например: ПК, торговые терминалы, веб-камеры и сетевое хранилище данных).

По способу связи они бывают:

- проводные;
- беспроводные.

Основные проблемы компьютерных сетей связаны с передачей данных. Скорость и надежность передачи данных во многом определяются расстоянием. Стоимость физических каналов, коммуникационного оборудования существенно влияет на общую стоимость сети. Поэтому основными классификационными признаками компьютерных сетей являются пространственные характеристики территорий, которые они охватывают. В зависимости от территории, обслуживаемой сетью, компьютерные сети подразделяются:

- на локальные (ЛВС, LAN, Local Area Network);
- региональные (MAN, Metropolitan Area Network);
- глобальные (WAN, Wide Area Network или GAN, Global Area Network);
- корпоративные.

Глобальная вычислительная сеть объединяет абонентов, расположенных в различных странах, на разных континентах. Взаимодействие между абонентами такой сети осуществляется на базе кабельных линий связи, радиосвязи и систем спутниковой связи.

Региональная вычислительная сеть связывает абонентов внутри большого города, экономического региона, страны. Обычно расстояние между абонентами региональной вычислительной сети составляет десятки, сотни километров.

Локальная вычислительная сеть (ЛВС) включает абонентов, расположенных в пределах небольшой территории. К классу локальных вычислительных сетей относятся сети отдельных предприятий, фирм, банков и т.д. Протяженность такой сети обычно ограничена пределами 2 - 2,5 км.

Объединение глобальных, региональных и локальных вычислительных сетей позволяет создавать многосетевые иерархии, обеспечивающие мощные средства обработки огромных информационных массивов и доступ к неограниченным информационным ресурсам. Локальные сети могут входить как компоненты в состав региональных и глобальных сетей, и наконец, глобальные сети могут образовывать сложные структуры.

Из глобальных наиболее популярна сеть Internet. В ее состав входит множество свободно соединенных сетей, причем каждая внутренняя сеть может обладать собственной структурой и способами управления. Основными ячейками Internet являются локальные вычислительные сети (рис. 2).

В состав Сети входит **абонент** (узел, хост, станция) - устройство, подключенное к сети и активно участвующее в информационном обмене. Узлами КС могут быть:

- компьютеры;
- сетевые устройства;
- другие устройства с доступом в сеть.

Рис. 2. **Пример вычислительной сети**

Абонентом также называют человека, пользователя:

- как активного участника сети;
- как конечный пункт доставки информации по сети;
- как участника правовых отношений.

Коммутация - установление связи между абонентами сети, одно из основных отличий современных компьютерных сетей от традиционных (телефонных, радио, телевизионных).

Основные методы коммуникации - это:

- коммутация каналов (телефонная сеть);
- коммутация пакетов (компьютерная сеть).

Техника коммутации была специально разработана для эффективной передачи компьютерного трафика (трафик - объем данных, принимаемых или передаваемых сетевым устройством). Первые шаги на пути создания компьютерных сетей на основе техники коммутации каналов показали, что этот вид коммутации не позволяет достичь высокой общей пропускной способности сети. Типичные сетевые приложения ге-

нерируют трафик очень неравномерно, с высоким уровнем пульсации скорости передачи данных. Например, при обращении к удаленному файловому серверу пользователь сначала просматривает содержимое каталога этого сервера, что порождает передачу небольшого объема данных. Затем он открывает требуемый файл в текстовом редакторе, и эта операция может создать достаточно интенсивный обмен данными, особенно если файл содержит объемные графические включения. После отображения нескольких страниц файла пользователь некоторое время работает с ними локально, что вообще не требует передачи данных по Сети, а затем возвращает модифицированные копии страниц на сервер - и это снова порождает интенсивную передачу данных по Сети.

Коэффициент *пульсации трафика* отдельного пользователя Сети, равный отношению средней интенсивности обмена данными к максимально возможной, может достигать 1:50 или даже 1:100. Если для описанной сессии организовать коммутацию канала между компьютером пользователя и сервером, то большую часть времени канал будет простаивать. В то же время коммутационные возможности Сети будут закреплены за данной парой абонентов и будут недоступны другим пользователям Сети.

При коммутации *пакетов* все передаваемые пользователем сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые *пакетами*. Сообщением называется логически завершенная порция данных - запрос на передачу файла, ответ на этот запрос, содержащий весь файл, и т.д. Сообщения могут иметь произвольную длину - от нескольких байт до многих мегабайт. *Пакеты* обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт.

При коммутации пакетов пользовательские данные (сообщения) перед началом передачи разбиваются на короткие пакеты фиксированной длины. Каждый пакет снабжается протокольной информацией (заголовком): коды начала и окончания пакета, адреса отправителя и получателя, номер пакета в сообщении, информация для контроля достоверности передаваемых данных в промежуточных узлах связи и в пункте назначения (контрольная сумма). Будучи независимыми единицами информации, пакеты, принадлежащие одному и тому же блоку информации, могут передаваться одновременно по различным маршрутам. Управление передачей и обработкой пакетов в узлах связи осуществляется коммутаторами или коммуникационными компьютерами. Одним из показателей этого метода является возможность согласования скоростей передачи данных между пунктами отправления и назначения, что обеспечивается наличием в сети эффективных развязок, реализуемых созданием буферных запоминающих устройств (ЗУ) в уз-

лах связи. Пакеты доставляются в пункт назначения с минимальной задержкой, где из них формируется первоначальное сообщение.

Технология коммутации пакетов позволяет:

- увеличить количество подключаемых узлов, так как здесь легче преодолеть трудности, связанные с подключением к коммутаторам дополнительных линий связи;
- осуществить альтернативную маршрутизацию (в обход поврежденных или занятых узлов связи и каналов), что создает повышенные удобства для пользователей;
- существенно сократить время на передачу пользовательских данных, повысить пропускную способность сети и эффективность использования сетевых ресурсов.

Одной из концепций коммутации пакетов является мультиплексирование с помощью разделения времени использования одного и того же канала многими пользователями, что повышает эффективность функционирования сети. Логика коммутации пакетов позволяет мультиплексировать многие пользовательские сеансы на один порт компьютера. Пользователь воспринимает порт как выделенный, в то время как он используется как разделенный ресурс. Мультиплексирование порта и канала называют виртуальным каналом. Коммутация пакетов и мультиплексирование обеспечивают сглаживание асимметричных потоков в каналах связи.

При коммутации пакетов в сети находятся пакеты разных пользователей, которые доставляются коммуникационным оборудованием до адресатов. На рис. 3 представлены схемы коммутации каналов и коммутации пакетов.

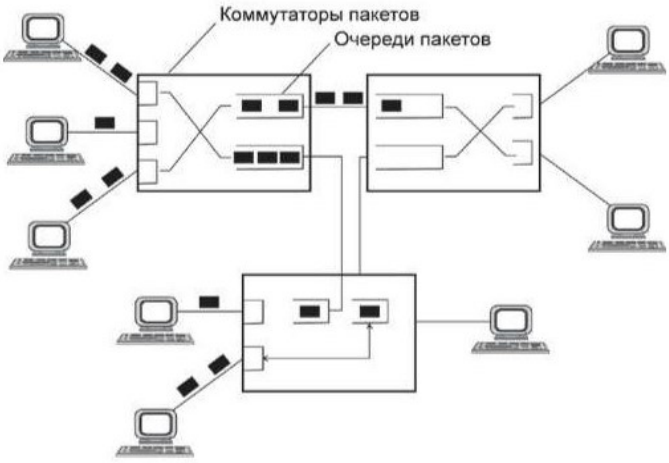

Рис. 3. **Схемы коммутации каналов и пакетов**

Достоинства и недостатки любой сетевой технологии относительны. В определенных ситуациях на первый план выходят достоинства, а недостатки становятся несущественными. Так, техника коммутации каналов хорошо работает в тех случаях, когда нужно передавать только трафик телефонных разговоров. Здесь с невозможностью "вырезать" паузы из разговора и более рационально использовать магистральные физические каналы между коммутаторами можно мириться. А вот при передаче очень неравномерного компьютерного трафика эта нерациональность уже выходит на первый план.

Первые научные работы о принципах работы сетей с коммутацией пакетов относятся к началу 1960-х гг. Исследования в области сетей с коммутацией пакетов стали основой, на которой базируются сегодняшняя сеть Internet и все другие вычислительные сети. Через некоторое время эти исследования вылились в исследовательскую программу Advanced Projects Research Agency (ARPAnet), в рамках которой была создана первая сеть с коммутацией пакетов, известная как ARPAnet. В 1972 г. был разработан первый протокол передачи данных между компьютерами, который назывался Network Control Protokol (NCP). После того как сетевые концепции были отработаны на ARPAnet, стали появляться другие компьютерные сети. Среди них ALOHAnet, Telenet, Transpac и др. Это были глобальные сети. История компьютерных сетей начинается именно с глобальных сетей. Но в 1972 г. Роберт Меткалф, работавший в фирме Xerox, разработал принципы Ethernet - сетей, которые впоследствии охватили весь мир, породив неизмеримое количество локальных сетей. Сети активно развивались, и в 1983 г. увидел свет стандарт протоколов стека TCP/IP. Он заменил применявшийся в ARPAnet протокол NCP, появилась система доменных имен DNS. С того времени развитие IP-сетей стало набирать мощь, этот процесс продолжается и сегодня.

Один из важных критериев классификации сетей - классификация по модели. Рассмотрим модель **клиент-сервер.** Под сервером понимают:

1) узловой компьютер в сети, предоставляющий свои услуги и сервисы другим, т.е. выполняющий определенные функции по запросам пользователей сети;

2) программа-сервер, устанавливаемая на компьютере-сервере.

Обслуживаемые компьютеры общаются с сервером посредством соответствующей клиент-программы, предназначенной для работы в паре с программой-сервером. Клиент-программа работает непосредственно на рабочей станции, т.е. на сетевом компьютере, с которого пользователь имеет доступ к сетевым сервисам и ресурсам.

Под клиентом понимаются:

- пользователь;
- прикладная программа, работающая в интересах пользователя для предоставления определенных услуг с сервера в какой-либо сети.

Клиент-сервер - это технология работы различных программ в сети. Программа, работающая по такой схеме, состоит из двух взаимодействующих частей: клиента и сервера. Сервер по командам клиента выполняет определенные действия, предоставляя услуги клиенту. То есть для предоставления услуг в такой схеме необходимы наличие и одновременная слаженная работа обеих указанных частей. По уровню управления локальные сети делятся на ***одноранговые и двуранговые.***

Одноранговые сети. В такой сети нет единого центра управления взаимодействием рабочих станций и нет единого устройства для хранения данных. Сетевая операционная система распределена по всем рабочим станциям. В одноранговой сети (peer-to-peer network) все компьютеры равноправны - каждый из компьютеров может быть и сервером, и клиентом. Пользователь каждого из компьютеров сам решает, какие ресурсы будут предоставлены в общее пользование и кому.

Компьютеры в одноранговых сетях организуются в рабочие группы (workgroups). Одноранговые сети, как правило, небольшие - расстояние по кабелю от 2 до 10 компьютеров. В такой сети обычно нет лица, ответственного за настройку и поддержку политики безопасности сети - администратора (network administrator). В одноранговой сети каждый пользователь ведет свою собственную политику безопасности, определяя, каким образом другие пользователи могут использовать его ресурсы, находящиеся в сетевом доступе. *Политика безопасности* (security policy) - это совокупность настроек, определяющая права пользователей сети на доступ к общим ресурсам. По мере добавления новых компьютеров в рабочую группу она становится трудно управляемой, так как управление политикой безопасности децентрализовано. Примером операционных систем для одноранговых сетей выступают все версии WINDOWS 9X, WINDOWS 2000, WINDOWS XP.

К достоинствам таких сетей можно отнести низкую стоимость и высокую надежность. Их недостатками являются:

- слабая защита информации;
- сложность управления сетью;
- зависимость эффективности работы от числа станций.

Двуранговые сети (сети клиент/сервер). Наиболее характерная особенность сети клиент/сервер - централизованное управление сетью. Такая сеть имеет хотя бы один выделенный сервер, который управляет пересылкой сообщений между объектами сети и всеми связями между сетевыми устройствами, хранит разделяемые информационные ресурсы, управляет политикой безопасности. На нем устанавливается серверное ядро сетевой операционной системы. Как правило, сервер - это самый мощный компьютер специального серверного исполнения, имеющий при необходимости высоконадежную внешнюю память (RAID-массивы).

Модель "клиент-сервер" значительно упрощает задачи администрирования сети, однако требует специалиста, который будет поддерживать работу сети. Сеть клиент/сервер обладает большей безопасностью, чем одноранговая сеть. Чтобы зарегистрироваться в системе, пользователь должен знать свои учетные данные (имя пользователя и пароль), созданные на сервере. Когда пользователь успешно зарегистрировался, он автоматически получает доступ ко всем ресурсам сети, на которые у него есть права. Сетевой администратор может присвоить права доступа как отдельному пользователю, так и группе пользователей.

Достоинства сети с выделенным сервером:

- надежная система защиты информации;
- высокое быстродействие;
- простота управления;
- отсутствие ограничений на число рабочих станций.

Недостатком таких сетей является их высокая стоимость.

Примером операционных систем для двуранговых сетей являются все версии WINDOWS NT, WINDOWS 2000/2003 Server фирмы Microsoft, а также операционная система Novell Net Ware фирмы Novell.

1.2. Типы серверов

Широкий выбор серверных систем требует от специалистов грамотно оценивать их вычислительную мощность, масштабируемость, надежность и степень готовности. Они должны четко сформулировать требования к серверам, изучить возможности поддержки, а также определить будущие затраты на модернизацию. Кроме того, надо хорошо ориентироваться в разнообразии предлагаемой на рынке продукции.

Серверы можно классифицировать, например, как по классу решаемых задач, так и по количеству обслуживаемых клиентов. В соответствии со вторым подходом различают серверы масштаба рабочей группы (workgroup), отдела (department), средних организаций (midrange), предприятия (enterprise).

Поскольку в рамках каждого типа конфигурация серверов значительно варьируется, четких границ между ними установить нельзя. Мощные компьютеры младшего класса могут выполнять роль серверов начального уровня в старшем смежном классе и наоборот.

Классификаций серверов существует довольно много, причем все они в той или иной степени перекрываются степенью работы. Так, фирмы-производители часто подразделяют выпускаемые серверы по типу исполнения: сверхтонкие (blade), классические напольные (tower), предназначенные для установки в стойки (rack) и с высокой степенью масштабируемости (super scalable). Сверхтонкие компьютеры позволяют не только экономить место, отводимое под каждый сервер, но и уменьшать энергопотребление. Напольные серверы обеспечивают высокую гибкость при размещении компонентов в корпусе и легко наращиваемы. Серверы для установки в стойку предназначены для консолидации серверных систем в центрах обработки данных и использования с внешними подсистемами памяти. Они могут эффективно применяться для кластерных решений, когда сами серверы, внешняя память и дополнительные устройства размещаются в одних и тех же стойках. Серверы с высокой степенью масштабируемости обычно предназначены для крупных предприятий и способны обеспечить решение практически любых задач корпорации.

Ниже приведены самые распространенные типы серверов, классифицируемых по классу решаемых задач.

Серверы приложений. Сервер приложений - сервер, предназначенный для выполнения прикладных процессов. Сервер приложений взаимодействует с клиентами, получая задания, и взаимодействует с базами данных, выбирая данные, необходимые для обработки. Для сервера приложений характерны расширенные возможности обработки информации, а взаимодействие с клиентом становится подобным работе приложения.

Серверы баз данных. Серверы баз данных используются для размещения и обслуживания централизованных баз банных, предназначенных для обработки пользовательских запросов. Модель "сервер базы данных" - архитектура вычислительной сети типа клиент-сервер, в которой пользовательский интерфейс и логика приложений сосредоточены на машине-клиенте, а информационные функции

(функции СУБД) - на сервере. Обычно клиентский процесс посылает запрос серверу на языке SQL. Ключевая характеристика сервера баз данных - его способность быстро извлекать и форматировать данные. Решающую роль в этом играют вычислительная мощность и масштабируемость системы. Понятия *сервер приложений* и *сервер баз данных* похожи, но в литературе по информационным технологиям встречаются оба эти понятия.

Файл-серверы. Файл-сервер обеспечивает взаимодействие между сетевыми станциями и дает пользователям доступ к файлам, которые необходимы им для работы. Кроме того, файл-сервер обычно ограничивает несанкционированный доступ к данным. Разница между файл-сервером и сервером приложений заключается в том, что первый хранит программы и данные, а второй выполняет программы и обрабатывает данные**.**

Почтовые серверы. Почтовые серверы занимаются входящими и исходящими сообщениями. Одна из задач почтового сервера - чтение адресов входящих сообщений и доставка корреспонденции в соответствующие почтовые ящики в пределах сети. В зависимости от развитости почтового сервера он может предоставлять администратору большую или меньшую степень контроля над локальными почтовыми ящиками, типами и размерами сообщений, которые они в состоянии получать, автоматическими ответами, которые можно составлять, и т.п.

Принт-серверы. Такие серверы позволяют всем подключенным к сети компьютерам распечатывать документы на одном или нескольких общих принтерах. В этом случае отпадает необходимость комплектовать каждый компьютер собственным печатающим устройством. Кроме того, принимая на себя все заботы о выводе документов на печать, принт-сервер освобождает компьютеры для другой работы. Например, принт-сервер хранит посланные на печать документы на своем жестком диске, выстраивает их в очередь и выводит на принтер в порядке очередности.

Серверы удаленного доступа. Эти системы позволяют связываться с офисной сетью по кабельным каналам связи и в беспроводных сетях. Находясь с ноутбуком где-нибудь вдали от офиса, всегда можно получить нужный файл, проверить, не пришла ли электронная почта, словом, получить любую необходимую информацию. При наличии хороших каналов связи разница между работой в офисе и вне его в этом случае практически незаметна.

Факс-серверы. Факс-сервер подобен упоминавшемуся ранее почтовому серверу. Оба эти типа серверов представляют собой мосты между исходящими и входящими сообщениями, оба должны направлять

входящие сообщения по указанному адресу. В случае почтовых серверов - это всегда почтовый ящик конкретного пользователя. В случае факс-серверов подразумевается, что принимающий сообщение компьютер и является местом назначения, поэтому модель почтового ящика здесь не работает. С другой стороны, факс-серверы, предназначенные для корпоративного использования, имеют некоторые параллели с моделью сервера электронной почты, обеспечивая доставку входящих факсов по конкретным адресам, присвоенным пользователям.

Серверы Internet. Сюда относятся серверы глобальной сети, обеспечивающие размещение сервисов сети разного типа, а также сетевые службы, обеспечивающие функционирование Internet совместно с ЛВС. Основные из них рассматриваются ниже. Применение вычислительных сетей дает следующие преимущества:

- совместное использование информации (например, файлов);
- совместное использование аппаратных средств (например, принтера, модема и др.);
- совместное использование программных ресурсов (например, программы типа клиент-сервер);
- обеспечение единой политики безопасности для узлов сети (например, настройка безопасности рабочих станций на сервере при подключении локальной сети к Internet);
- разграничение полномочий узлов сети (например, для распределения полномочий между различными подразделениями предприятия);
- обеспечение защиты информации совместного использования (например, резервное копирование на стороне сервера);
- обеспечение эффективных средств взаимодействия пользователей друг с другом (например, посредством электронной почты. Возможно проведение конференций, форумов и др.);
- повышение надежности всей информационной системы, поскольку при отказе одной ЭВМ другая, резервная, может взять на себя ее функции и рабочую нагрузку.

1.3. Модель взаимодействия открытых систем (OSI)

Из того, что протокол является соглашением, принятым двумя взаимодействующими объектами, в данном случае двумя работающими в сети компьютерами, совсем не следует, что он обязательно

представляет собой стандарт. Но на практике при реализации сетей стремятся использовать стандартные протоколы. Это могут быть фирменные, национальные или международные стандарты.

Международная Организация по Стандартам (International Standards Organization, ISO) разработала модель, которая четко определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какую работу должен делать каждый уровень. Эта модель называется моделью взаимодействия открытых систем (Open System Interconnection, OSI), или моделью ISO/OSI.

В модели OSI взаимодействие делится на семь уровней (слоев) (рис. 4). Каждый уровень имеет дело с одним определенным аспектом взаимодействия. Таким образом, проблема взаимодействия декомпозирована на семь частных проблем, каждая из которых может быть решена независимо от других. Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями.

Модель содержит семь уровней. Основная идея модели заключается в том, что каждому уровню отводится конкретная роль. Поэтому общая задача передачи данных формализуется и расчленяется на отдельные легко обозримые задачи. В процессе развития и совершенствования любой системы возникает потребность изменения отдельных компонентов, а так как интерфейсы между уровнями определены однозначно, можно изменить функции одного или нескольких из них, сохраняя возможность безошибочной работы сети в целом. В сетях происходит взаимодействие между одноименными уровнями модели в различных ЭВМ. Такое взаимодействие должно выполняться по определенным правилам, называемым протоколом.

Большинство сетей реализует все семь уровней. Однако в режиме потока информации некоторые реализации сетей пропускают один или более уровней. При этом функции отсутствующих уровней распределяются между другими уровнями. Два самых низших уровня OSI реализуются аппаратным и программным обеспечением; остальные пять высших уровней, как правило, реализуются программным обеспечением.

Справочная модель OSI описывает, каким образом информация проделывает путь через среду сети (например, провода) от одной прикладной программы до другой, находящейся в другом компьютере.

Задача каждого уровня - предоставление услуг вышележащему уровню, маскируя детали реализации этих услуг. При этом каждый уровень работает так, как будто он напрямую связан с таким же уровнем на другом компьютере. Это логическая, или виртуальная,

связь между одинаковыми уровнями. Физическая связь через среду передачи данных существует только на физическом уровне. Перед подачей в сеть данные разбиваются на пакеты. Пакет проходит от верхнего седьмого уровня (прикладной, или уровень приложений) последовательно через все уровни программного обеспечения, и на каждом уровне к пакету добавляется некоторая управляющая (форматирующая, или адресная) информация, называемая ***заголовком***, необходимая для успешной передачи данных по сети. Модель ISO/OSI представлена на рис.4.

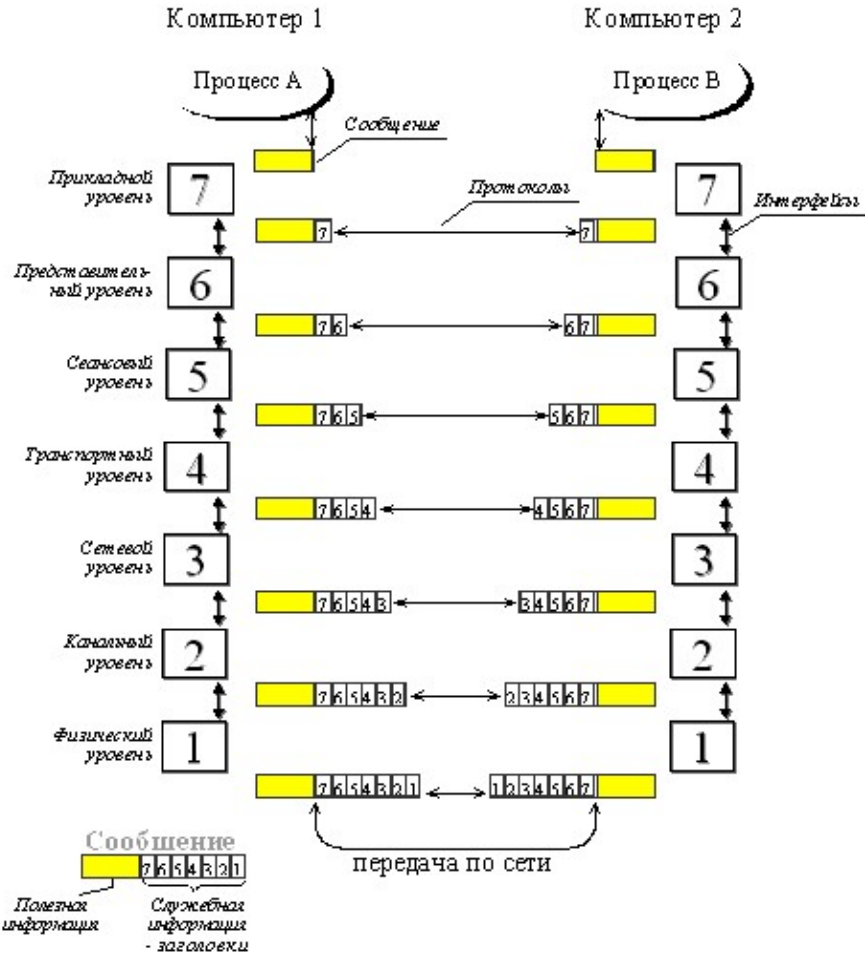

Рис. 4. **Модель взаимодействия открытых систем ISO/OSI**

Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. Следует иметь в виду, что приложение может взять на себя функции некоторых верхних уровней модели OSI, в таком случае при необходимости межсетевого обмена оно обращается напрямую к системным средствам, выполняющим функции оставшихся нижних уровней модели OSI.

Приложение конечного пользователя может применять системные средства взаимодействия не только для организации диалога с другим приложением, выполняющимся на другой машине, но и просто для получения услуг того или иного сетевого сервиса, например, доступа к удаленным файлам, получение почты или печати на разделяемом принтере.

Итак, пусть приложение обращается с запросом к прикладному уровню, например к файловому сервису. На основании этого запроса программное обеспечение прикладного уровня формирует сообщение стандартного формата, в которое помещает служебную информацию (заголовок) и, возможно, передаваемые данные. Затем это сообщение направляется представительному уровню. Представительный уровень добавляет к сообщению свой заголовок и передает результат вниз сеансовому уровню, который, в свою очередь, добавляет свой заголовок, и т.д. Некоторые реализации протоколов предусматривают наличие в сообщении не только заголовка, но и концевика. Наконец, сообщение достигает самого низкого, физического, уровня, который действительно передает его по линиям связи.

Когда сообщение по сети поступает на другую машину, оно последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует, обрабатывает и удаляет заголовок своего уровня, выполняет соответствующие данному уровню функции и передает сообщение вышележащему уровню.

Кроме термина "сообщение" (message), существуют и другие названия, используемые сетевыми специалистами для обозначения единицы обмена данными. В стандартах ISO для протоколов любого уровня применяется такой термин, как "протокольный блок данных" - Protocol Data Unit (PDU). Кроме того, часто используются названия "кадр" (frame), "пакет" (packet), "дейтаграмма" (datagram).

Физический уровень. Этот уровень имеет дело с передачей битов по физическим каналам, таким, например, как коаксиальный кабель, "витая пара" или оптоволоконный кабель. К этому уровню имеют отношение характеристики физических сред передачи данных: полоса пропускания, помехозащищенность, волновое сопротив-

ление и др. На этом же уровне определяются характеристики электрических сигналов, такие как требования к фронтам импульсов, уровням напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме того, здесь стандартизуются типы разъемов и назначение каждого контакта.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

Примером протокола физического уровня может служить спецификация 10Base-T технологии Ethernet, которая определяет в качестве используемого кабеля неэкранированную "витую пару" категории 3 с волновым сопротивлением 100 ом, разъемом RJ-45, максимальную длину физического сегмента 100 м, манчестерский код для представления данных на кабеле и другие характеристики среды и электрических сигналов.

Канальный уровень. На физическом уровне просто пересылаются биты. При этом не учитывается, что в некоторых сетях, в которых линии связи используются (разделяются) попеременно несколькими парами взаимодействующих компьютеров, физическая среда передачи может быть занята. Поэтому одной из задач канального уровня выступает проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит в начало и конец каждого кадра, чтобы отметить его, а также вычисляет контрольную сумму, складывая все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка.

В протоколах канального уровня, используемых в локальных сетях, заложены определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это делает только в сети с совершенно определенной топологией связей, именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда. Примерами протоколов канального уровня являются протоколы Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень обеспечивает обмен сообщениями между двумя соседними компьютерами, соединенными индивидуальной линией связи. Примерами протоколов "точка - точка" (как часто называют такие протоколы) могут служить широко распространенные протоколы PPP и LAP-B.

Сетевой уровень. Этот уровень служит для образования единой транспортной системы, объединяющей несколько сетей с различными принципами передачи информации между конечными узлами. Рассмотрим функции сетевого уровня на примере локальных сетей. Протокол канального уровня локальных сетей обеспечивает доставку данных между любыми узлами только в сети с соответствующей типовой топологией. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами. Для того чтобы, с одной стороны, сохранить простоту процедур передачи данных для типовых топологий, а с другой стороны, допустить использование произвольных топологий, применяется дополнительный сетевой уровень. На этом уровне вводится понятие "сеть". В данном случае под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Таким образом, внутри сети доставка данных регулируется канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень.

Сообщения сетевого уровня принято называть пакетами (packets). При организации доставки пакетов на сетевом уровне используется понятие "номер сети". В этом случае адрес получателя состоит из номера сети и номера компьютера в этой сети.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Маршрутизатор - это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое

количество транзитных передач (hops) между сетями, каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является главной задачей сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута служит время передачи данных по этому маршруту, оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.

На сетевом уровне выделяются два вида протоколов. Первый вид относится к определению правил передачи пакетов с данными конечных узлов от узла к маршрутизатору и между маршрутизаторами. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. К сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

Примерами протоколов сетевого уровня являются протокол межсетевого взаимодействия IP стека TCP/IP и протокол межсетевого обмена пакетами IPX стека Novell.

Транспортный уровень. На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням стека - прикладному и сеансовому - передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное - способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких, чем транспортный, уровней, а с другой стороны, этот выбор зависит от того, насколько надежной является вся система транспортировки данных в сети. Так, например, если качество каналов передачи связи очень высокое и вероятность возникновения ошибок, не обнаруженных протоколами более низких уровней, невелика, то разумно воспользоваться одним из облегченных сервисов транспортного уровня, не обремененных многочисленными проверками, квитированием и другими приемами повышения надежности. Если же транспортные средства изначально очень ненадежны, то целесообразно обратиться к наиболее развитому сервису транспортного уровня, который работает, используя максимум средств для обнаружения и устранения ошибок, с помощью предварительного установления логического соединения, контроля доставки сообщений с помощью контрольных сумм и циклической нумерации пакетов, установления тайм-аутов доставки и т.п.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети - компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell.

Сеансовый уровень. Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент, а также предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того чтобы начинать все с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется.

Уровень представления. Этот уровень обеспечивает гарантию того, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе. При необходимости уровень представления выполняет преобразование форматов данных в некоторый общий формат представления, а на приеме, соответственно, выполняет обратное преобразование. Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. На этом уровне могут выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером

протокола, работающего на уровне представления, является протокол Secure Socket Layer (SSL), который способствует секретному обмену сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень. Прикладной уровень - это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).

Существует большое разнообразие протоколов прикладного уровня. Приведем в качестве примеров хотя бы несколько наиболее распространенных реализаций файловых сервисов: NCP в операционной системе Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP и TFTP, входящие в стек TCP/IP.

Модель OSI представляет хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, сервисами, предоставляемыми на верхних уровнях, и прочими параметрами.

1.4. Протоколы взаимодействия приложений и протоколы транспортной подсистемы

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня - физический, канальный и сетевой - являются сетезависимыми, т.е. протоколы этих уровней тесно связаны с технической реализацией сети, с используемым коммуникационным оборудованием. Например, переход на оборудование FDDI означает полную смену протоколов физического и канального уровня во всех узлах сети.

Три верхних уровня - сеансовый, уровень представления и прикладной - ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют никакие изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Так, переход от Ethernet

на высокоскоростную технологию ATM не потребует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних уровней. Это позволяет разрабатывать приложения, не зависящие от технических средств, непосредственно занимающихся транспортировкой сообщений.

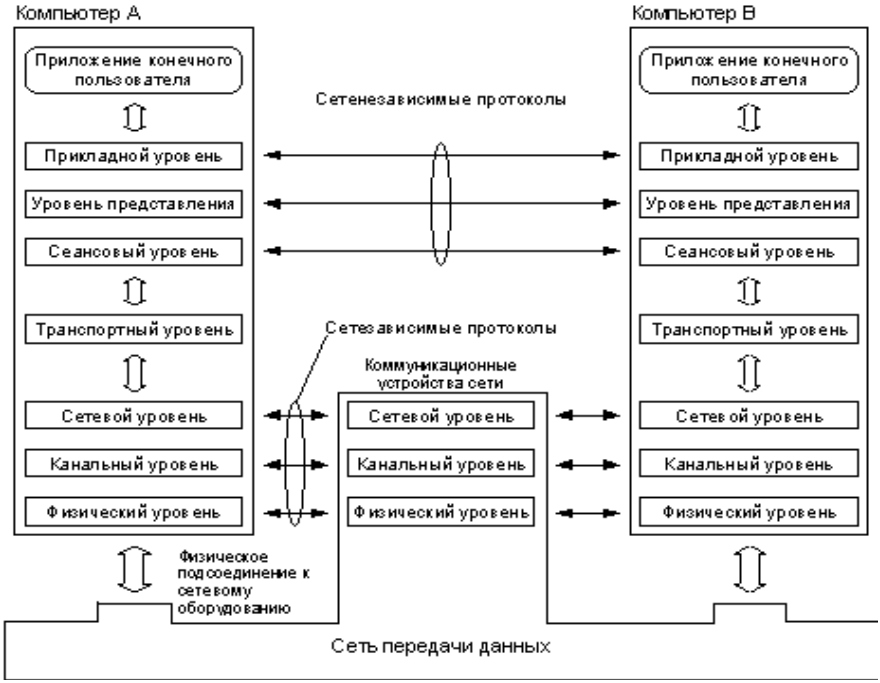

Рис. 5. **Сетезависимые и сетенезависимые уровни модели OSI**

На рис. 5 показаны уровни модели OSI, на которых работают различные элементы сети. Компьютер с установленной на нем сетевой ОС взаимодействует с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство может работать либо только на физическом уровне (повторитель), либо на физическом и канальном (мост и коммутатор), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (маршрутизатор).

2. ОРГАНИЗАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

2.1. Сетевое оборудование

Оборудование, с помощью которого осуществляется объединение компьютеров в сети, называется сетевым оборудованием. По способу участия в передаче данных сетевое оборудование подразделяется на пассивное и активное.

Пассивное оборудование работает только с электрическими сигналами, не анализируя при этом информацию из передаваемых данных. К пассивному сетевому оборудованию относятся кабели, соединительные разъемы, коммутационные панели, повторители (усилители) и др.

Активное оборудование читает и анализирует информацию из передаваемых данных и на основании этой информации принимает решение об их дальнейшей передаче. К активному оборудованию относятся сетевые адаптеры, коммутаторы, маршрутизаторы и другое оборудование.

Сетевой адаптер - это плата, с помощью которой компьютер подключается к локальной сети. Выбор платы сетевого адаптера зависит от разных факторов: протокола канального уровня (наиболее часто используется Ethernet, но могут быть применены адаптеры, поддерживающие Token Ring, FDDI, ATM и др.), скорости передачи по сети (Ethernet имеет 10 Мбит/с, Fast Ethernet - 100 Мбит/с, Gigabit Ethernet - 1000 Мбит/с), типа сетевого кабеля. Тип сетевого кабеля выбирается в то же время, что и протокол канального уровня, поскольку приобретаемый адаптер должен поддерживать соответствующую среду передачи данных. Некоторые протоколы канального уровня рассчитаны на разные типы кабеля, и для каждого типа есть свои сетевые адаптеры. Также есть протоколы, разработанные для использования только одного типа кабеля: типа системной шины, в которую вставляется плата адаптера (обычно PCI), аппаратных ресурсов, запрашиваемых адаптером. Плата сетевого адаптера нуждается в свободной линии запроса на прерывание (IRQ, interrupt request line) и обычно в адресе порта ввода/вывода или адресе памяти либо в том и другом. Когда оцениваются сетевые адаптеры, необходимо учитывать требования адаптера к ресурсам и сами доступные ресур-

сы компьютера. Если на ПК работает технология Plug and Play, то компьютер сам динамически назначает аппаратные ресурсы адаптеру, класс компьютера, использующего сетевой адаптер: сервер/рабочая станция, домашний/офисный. Функции сетевых адаптеров на серверах и рабочих станциях одинаковы, но есть сетевые платы, специально предназначенные для подключения к серверам.

Репитер (повторитель) - это устройство для усиления сигналов в Сети в том случае, если длина сегмента сети превышает допустимую. В современной сети очень редко можно увидеть отдельно стоящий репитер. Как правило, его функции встроены в другое устройство - концентратор или коммутатор.

Концентратор - это устройство, выполняющее функции связующего звена для кабеля в сети с топологией "звезда". Каждый компьютер отдельным кабелем подключен к центральному концентратору. Концентратор распространяет трафик, пришедший на любой из портов, через все остальные порты. В зависимости от кабеля в концентраторе могут быть применены электрические схемы, оптические компоненты или другие технологии для распределения входящего сигнала между всеми выходными портами. Внешне концентратор представляет собой коробку с пронумерованными портами, к которым подключается кабель. Концентраторы бывают пассивные и активные (ретранслирующие) с функциями усиления сигналов.

Коммутатор - это многопортовое устройство, у которого каждый порт связан с отдельным сегментом сети. Внешне похожий на концентратор, коммутатор принимает входящий трафик через свои порты, но в отличие от концентратора, который передает исходящий трафик через множество портов, коммутатор передает трафик только через один порт, необходимый для достижения места назначения. Основная роль коммутаторов состоит в коммутации каналов, заключающейся в соединении на своих внутренних шинах входных и выходных цепей в зависимости от того, куда направляются данные. Иногда коммутация осуществляется с помощью буферов, без непосредственного электрического соединения.

Применение коммутаторов позволяет соединить вместе несколько сетей и воспользоваться преимуществами связи без помех, возникающих вследствие совместного использования полосы пропускания. В зависимости от местоположения коммутаторов в сети их можно использовать для изолирования частей сети на уровне рабочих групп или магистрали. Поэтому различают коммутаторы рабочих групп и магистральные коммутаторы.

Маршрутизатор (роутер) - это устройство, определяющее маршрут передачи пакетов в сети в соответствии с заданным адресом. Маршрутизаторы работают на сетевом уровне, поэтому они способны интегрировать разнородные сети. Например, соединить Ethernet и Token Ring. Выбор маршрутизатора зависит от протокола. Наиболее широко применяется Internet Protocol (IP, межсетевой протокол), лежащий в основе Internet. Маршрутизаторы изолируют трафик в отдельных ЛВС, передавая только пакеты, адресованные системам в других ЛВС.

Модем - это английское слово-неологизм, составленное из двух слов Modulator/Demodulator (модулятор/демодулятор). Модем преобразует цифровые данные, с которыми работает компьютер, в аналоговую форму, пригодную для передачи по телефонным линиям на значительные расстояния, и наоборот, аналоговые сигналы при приеме превращаются в цифровые, понятные компьютеру. Это последовательные устройства передачи данных, т.е. одновременно они передают или принимают один бит информации. Используется для подключения к Internet по телефонной линии. Основной характеристикой модема является скорость передачи.

2.2. Линии связи и каналы передачи данных

Для построения компьютерных сетей применяются линии связи, использующие различную физическую среду. В качестве физической среды в коммуникациях используются: металлы (в основном медь), сверхпрозрачное стекло (кварц) или пластик и эфир. Физическая среда передачи данных может представлять собой кабель "витая пара", коаксиальный кабель, волоконно-оптический кабель и окружающее пространство. Линии связи, или линии передачи данных, - это промежуточная аппаратура и физическая среда, по которой передаются информационные сигналы (данные). В одной линии связи можно образовать несколько каналов связи (виртуальных или логических каналов), например путем частотного или временного разделения каналов. Канал связи - это средство односторонней передачи данных. Если линия связи монопольно используется каналом связи, то в этом случае линию связи называют каналом связи. Канал передачи данных - это средство двухстороннего обмена данными, которые включают в себя линии

связи и аппаратуру передачи (приема) данных. Каналы передачи данных связывают между собой источники информации и приемники информации. В зависимости от физической среды передачи данных каналы связи можно разделить:

- на проводные линии связи без изолирующих и экранирующих оплеток;
- кабельные, где для передачи сигналов используются такие линии связи, как кабели "витая пара", коаксиальные кабели или оптоволоконные кабели;
- беспроводные (радиоканалы наземной и спутниковой связи), использующие для передачи сигналов электромагнитные волны, которые распространяются по эфиру.

2.2.1. Проводные линии связи

Проводные (воздушные) линии связи используются для передачи телефонных и телеграфных сигналов, а также для передачи компьютерных данных. Эти линии связи применяются в качестве магистральных линий связи. По проводным линиям связи могут быть организованы аналоговые и цифровые каналы передачи данных. Скорость передачи по проводным линиям "простой старой телефонной линии" (POST - Primitive Old Telephone System) является очень низкой. Кроме того, к недостаткам этих линий относятся помехозащищенность и возможность простого несанкционированного подключения к сети.

Кабельные линии связи имеют довольно сложную структуру. Кабель состоит из проводников, заключенных в несколько слоев изоляции. В компьютерных сетях используются три типа кабелей. "Витая пара" (twisted pair) - кабель связи, представляющий собой витую пару медных проводов (или несколько пар проводов), заключенных в экранированную оболочку. Пары проводов скручиваются между собой с целью уменьшения наводок. "Витая пара" является достаточно помехоустойчивой. Существует два типа этого кабеля: неэкранированная "витая пара" UTP и экранированная "витая пара" STP. Характерным для этого кабеля является простота монтажа. Данный кабель - самый дешевый и распространенный вид связи, который нашел широкое применение в самых распространенных локальных сетях с архитектурой Ethernet, построенных по топологии типа "звезда". Кабель подключается к сетевым устройствам при помощи соединителя RJ45 и используется для передачи данных на скорости 10 Мбит/с и

100 Мбит/с. "Витая пара" обычно применяется для связи на расстояние не более нескольких сот метров. К недостаткам кабеля "витая пара" можно отнести возможность простого несанкционированного подключения к сети.

Коаксиальный кабель (coaxial cable) - это кабель с центральным медным проводом, который окружен слоем изолирующего материала, чтобы отделить центральный проводник от внешнего проводящего экрана (медной оплетки или слоя алюминиевой фольги). Внешний проводящий экран кабеля покрывается изоляцией. Существует два типа коаксиального кабеля: тонкий коаксиальный кабель диаметром 5 мм и толстый коаксиальный кабель диаметром 10 мм. У толстого коаксиального кабеля затухание меньше, чем у тонкого. Стоимость коаксиального кабеля выше стоимости "витой пары", и выполнение монтажа сети сложнее, чем "витой парой". Коаксиальный кабель применяется, например, в локальных сетях с архитектурой Ethernet, построенных по топологии типа "общая шина". Коаксиальный кабель более помехозащищенный, чем "витая пара", и снижает собственное излучение. Пропускная способность - 50-100 Мбит/с. Допустимая длина линии связи - несколько километров. Несанкционированное подключение к коаксиальному кабелю сложнее, чем к "витой паре".

Оптоволоконный кабель (fiber optic) - это оптическое волокно на кремниевой или пластмассовой основе, заключенное в материал с низким коэффициентом преломления света, который закрыт внешней оболочкой. Оптическое волокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон. На передающем конце оптоволоконного кабеля требуется преобразование электрического сигнала в световой, а на приемном конце - обратное преобразование. Основное преимущество этого типа кабеля - чрезвычайно высокий уровень помехозащищенности и отсутствие излучения. Несанкционированное подключение очень сложно. Скорость передачи данных 3Гбит/с. Основные недостатки оптоволоконного кабеля - это сложность его монтажа, небольшая механическая прочность и чувствительность к ионизирующим излучениям.

2.2.2. Беспроводные каналы связи

Радиоканалы наземной (радиорелейной и сотовой) и спутниковой связи образуются с помощью передатчика и приемника радиоволн и относятся к технологии беспроводной передачи данных.

Радиорелейные каналы связи. Состоят из последовательности станций, являющихся ретрансляторами. Связь осуществляется в пределах прямой видимости, дальности между соседними станциями до 50 км. Цифровые радиорелейные линии связи (ЦРРС) применяются в качестве региональных и местных систем связи и передачи данных, а также для связи между базовыми станциями сотовой связи.

Спутниковые каналы связи. В спутниковых системах используются антенны СВЧ-диапазона частот для приема радиосигналов от наземных станций и ретрансляции этих сигналов обратно на наземные станции. В спутниковых сетях используются три основных типа спутников, которые находятся на геостационарных орбитах, средних или низких орбитах. Спутники запускаются, как правило, группами. Разнесенные друг от друга, они могут обеспечить охват почти всей поверхности Земли. Работа спутникового канала передачи данных представлена на рис. 6.

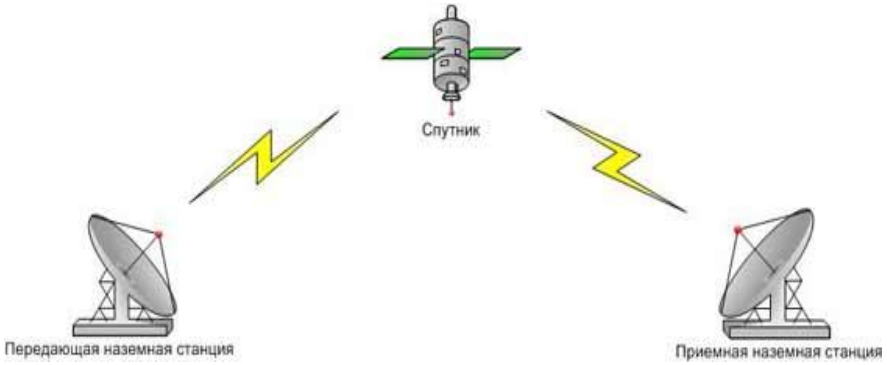

Рис. 6. **Работа спутникового канала передачи данных**

Целесообразнее использовать спутниковую связь для организации канала связи между станциями, расположенными на очень больших расстояниях, и возможности обслуживания абонентов в самых труднодоступных точках. Пропускная способность высокая - несколько десятков Мбит/с. Радиоканалы сотовой связи строятся по тем же принципам, что и сотовые телефонные сети. Сотовая связь - это беспроводная телекоммуникационная система, состоящая из сети наземных базовых приемопередающих станций и сотового коммутатора (или центра коммутации мобильной связи).

Базовые станции (БС) подключаются к центру коммутации, который обеспечивает связь как между базовыми станциями, так и с другими телефонными сетями и с глобальной сетью Internet. По вы-

полняемым функциям центр коммутации аналогичен обычной АТС проводной связи. LMDS (Local Multipoint Distribution System) - это стандарт сотовых сетей беспроводной передачи информации для фиксированных абонентов. Система строится по сотовому принципу (рис. 7), одна базовая станция позволяет охватить район радиусом несколько километров (до 10 км) и подключить несколько тысяч абонентов. Сами БС объединяются друг с другом высокоскоростными наземными каналами связи либо радиоканалами. Скорость передачи данных до 45 Мбит/с.

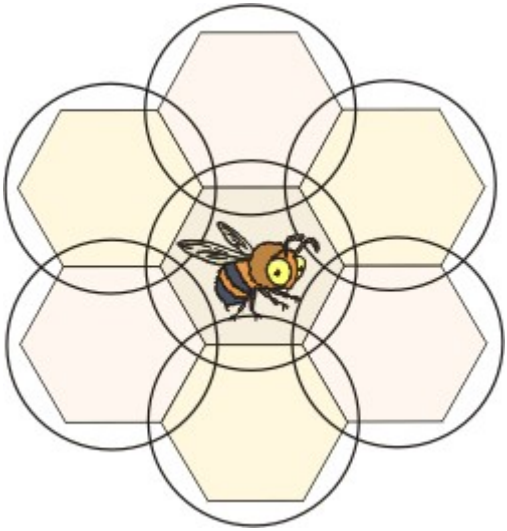

Рис. 7. **Схема расположения ячеек при сотовой связи**

Радиоканалы WiMAX (Worldwide Interoperability for Microwave Access) аналогичны Wi-Fi. WiMAX в отличие от традиционных технологий радиодоступа работает и на отраженном сигнале, вне прямой видимости базовой станции. Эксперты считают, что мобильные сети WiMAX открывают гораздо более интересные перспективы для пользователей, чем фиксированный WiMAX, предназначенный для корпоративных заказчиков. Информацию можно передавать на расстояние до 50 км со скоростью до 70 Мбит/с.

Радиоканалы MMDS (Multichannel Multipoint Distribution System) способны обслуживать территорию в радиусе 50-60 км, при этом прямая видимость передатчика оператора является не обязательной. Средняя гарантированная скорость передачи данных составляет 500 Кбит/с - 1 Мбит/с, но можно обеспечить до 56 Мбит/с на один канал.

Стандартом беспроводной связи для локальных сетей является технология Wi-Fi, которая обеспечивает подключение в двух режимах: точка-точка (для подключения двух ПК) и инфраструктурное соединение (для подключения нескольких ПК к одной точке доступа). Скорость обмена данными до 11 Мбит/с при подключении точка-точка и до 54 Мбит/с при инфраструктурном соединении.

Радиоканалы Bluetooht - это технология передачи данных на короткие расстояния (не более 10 м) и может быть использована для создания домашних сетей. Скорость передачи данных не превышает 1 Мбит/с.

2.3. Понятие топологии сети

Топология ЛВС - это усредненная геометрическая схема соединения узлов сети. Выбор той или другой топологии определяется областью применения и размером конкретной ЛВС, расположением ее узлов. С топологией сети связаны методы доступа к передающей среде и выбор сетевого оборудования.

Для ЛВС были разработаны несколько схем, включающих в себя аппаратные средства и протоколы передачи данных. Эти системы поддерживает соответствующее сетевое программное обеспечение. Система доступа к сети (аппаратура и протокол) обеспечивает электронную магистраль для передачи данных, а сетевая операционная система - управление ресурсами всей системы и обработкой данных.

Метод доступа определяет набор правил, используемых узлом сети для получения доступа к передающей среде. Рассмотрим методы доступа, применяемые в современных ЛВС. Множественный доступ с контролем несущей и обнаружением коллизий (конфликтов) базируется на алгоритме доступа CSMA/CD (Carrier Sensitive Multiple Access With Collision Detection), где все узлы имеют равные возможности доступа к сетевой среде. Перед передачей данных узел "прослушивает" среду и, если она свободна, начинает передачу. При одновременной попытке доступа к среде нескольких узлов фиксируется "столкновение", и сеанс передачи повторяется позднее. Иначе этот метод называется методом доступа Ethernet, или методом случайного доступа. По существу, метод доступа CSMA/CD предполагает широковещательную передачу кадров. Все рабочие станции логического сетевого сегмента прочитывают адресную часть передаваемой ин-

формации. Узел, адрес которого указан в кадре, принимает информацию. Метод разработан в 1975 г. фирмой Xerox и сначала использовался в сетях с шинной (магистральной) топологией.

Маркерное кольцо (Token Ring). Метод разработан фирмой IBM и рассчитан на кольцевую топологию сети. Этот принцип передачи данных в кольцевой сети носит название метода передачи маркера (token). Суть его такова. Маркер (уникальная последовательность битов) передается от одного компьютера к другому до тех пор, пока его не получит тот, который "хочет" передать данные. Передающий компьютер помещает кадр в маркер и посылает его по кольцу.

Данные проходят через несколько компьютеров, пока не достигнут того, чей адрес совпадает с адресом получателя, указанным в кадре. После этого принимающий компьютер посылает передающему узлу сообщение, в котором подтверждает прием данных. Получив подтверждение, передающий компьютер создает новый маркер и возвращает свободный маркер в сеть. Передача маркера не отнимает много времени и практически не влияет на пропускную способность сети.

Маркерная шина (метод доступа Arcnet). Разработан фирмой Datapoint Corporation и используется в топологиях "звезда" и общая шина. Маркер создается одной из станций сети и имеет адресное поле, где указывается адрес узла, владеющего маркером. Передачу осуществляет только узел, владеющий маркером, все остальные работают на прием. Последовательность передачи маркера от одной станции к другой определяется управляющей станцией сети. Станции, последовательно получающие маркер для передачи кадров, образуют "логическое кольцо". Станция, получившая маркер (полномочия на передачу информации), передает подготовленный кадр в шину. Если кадра для передачи нет, она посылает маркер другой станции согласно установленному порядку передачи полномочий. Станция назначения, получив маркер, "отцепляет" кадр от маркера и передает его следующей станции. Этот метод позволяет обеспечить приоритетное обслуживание абонентов.

Чтобы передать данные по кабелю или получить их из сети, платы сетевого интерфейса используют специфический метод доступа к кабелю. Международным институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers - IEEE) разработан одобренный Международной организацией по стандартизации (ISO) набор стандартов, являющихся частью стандарта OSI. Для локальных сетей предусмотрены следующие стандарты:

- 802.2 - Logical Link Control (LLC);

- 802.3 - CSMA/CD LAN (Ethernet);
- 802.4 - Token Bus LAN - маркерная шина;
- 802.5 - Token Ring LAN (IBM Token Ring) - маркерное кольцо.

Эти стандарты используются для определения физического уровня и уровня связи данных модели OSI. Уровень связи данных разделяется на логический подуровень Logical Link Control (LLC) и уровень метода управления носителем.

Уровень Logical Link Control обеспечивает единый стандартный интерфейс между верхними уровнями протокола и нижним уровнем Media Access Control (MAC). Уровень LCC аналогичен коммутационной панели, которая направляет потоки данных между нижним и верхним уровнями.

Среди топологических схем наиболее популярными являются:

- шинная (магистральная, общая шина);
- "звезда";
- "кольцо";
- многосвязная.

К первым трем типам топологии относятся 99 % всех локальных сетей.

Общая шина (BUS). В шинной топологии используется один кабель (в основном, тонкий коаксиальный), именуемый магистралью, или сегментом, к которому с помощью специальных коннекторов подсоединены все устройства сети (рис. 8).

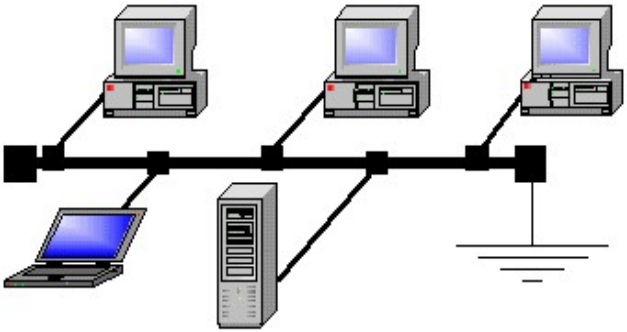

Рис. 8. **Шинная топология**

Данная топология относится к наиболее простым и широко распространенным топологиям. В сети с шинной топологией компьютеры адресуют данные конкретному компьютеру, передавая их по кабелю в виде электрических сигналов всем компьютерам сети; однако информацию принимает только тот, адрес которого соответствует

адресу получателя, указанному в кадре. Причем в каждый момент времени только один компьютер может вести передачу.

Так как данные в сеть передаются лишь одним компьютером, ее производительность зависит от количества компьютеров, подключенных к шине. Чем их больше, тем медленнее сеть. Однако вывести прямую зависимость между пропускной способностью сети и количеством компьютеров в ней нельзя, поскольку на быстродействие сети влияет множество факторов, в том числе:

- характеристики аппаратного обеспечения компьютеров в сети;
- частота, с которой компьютеры передают данные;
- тип работающих сетевых приложений;
- тип сетевого кабеля;
- расстояние между компьютерами в сети.

Шинная топология пассивна. Это значит, что компьютеры только слушают передаваемые по сети данные, но не участвуют в их перемещении от отправителя к получателю. Поэтому, если один из компьютеров выйдет из строя, это не скажется на работе остальных. В активных топологиях компьютеры регенерируют сигналы и передают их по сети.

Электрические сигналы распространяются по всей сети - от одного конца кабеля к другому. Если не предпринимать никаких специальных действий, сигнал, достигая конца кабеля, будет отражаться и не позволит другим компьютерам осуществлять передачу. Поэтому после того, как данные достигнут адресата, электрические сигналы необходимо погасить. Чтобы предотвратить отражение электрических сигналов, на каждом конце кабеля устанавливают специальные устройства - терминаторы (terminators), поглощающие эти сигналы.

"Кольцо" (Ring). Пример кольцевой топологии приведен на рис. 9.

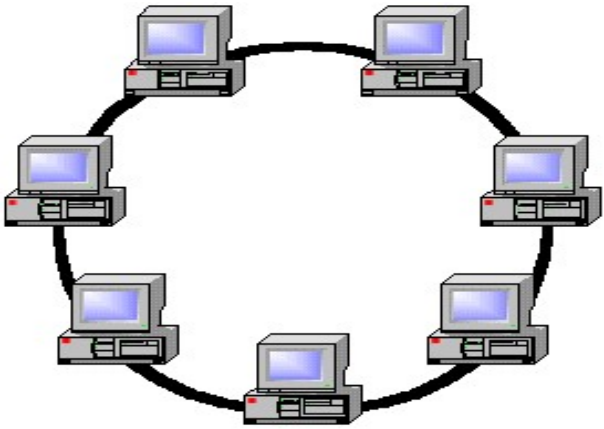

Рис. 9. **Топология "кольцо"**

При топологии "кольцо" компьютеры подключаются к кабелю, замкнутому в кольцо. Выход одного компьютера подключается к входу другого, каждый узел должен иметь два сетевых интерфейса. Сигналы передаются по кольцу в одном направлении и проходят через каждый компьютер. В отличие от пассивной шинной топологии здесь каждый компьютер выступает в роли репитера (повторителя), усиливая сигналы и передавая их следующему компьютеру. Поэтому, если выйдет из строя один компьютер, функционирование сети может нарушиться. В реальной ситуации этого не случается, поскольку подсоединение узла к кольцу выполняется специальным образом.

Для создания кольцевой топологии в основном используется волоконно-оптический кабель (сеть FDDI), но допустимо использование "витой пары" (Token Ring). Эта топология удобна для оптоволоконных каналов, где сигнал может передаваться только в одном направлении (но при наличии двух колец, как в FDDI, возможна и двунаправленная передача).

"Звезда" (Star). Это самая старая сетевая топология (рис. 10). При топологии "звезда" все компьютеры с помощью отдельных сегментов кабеля подключаются к одному центральному узлу.

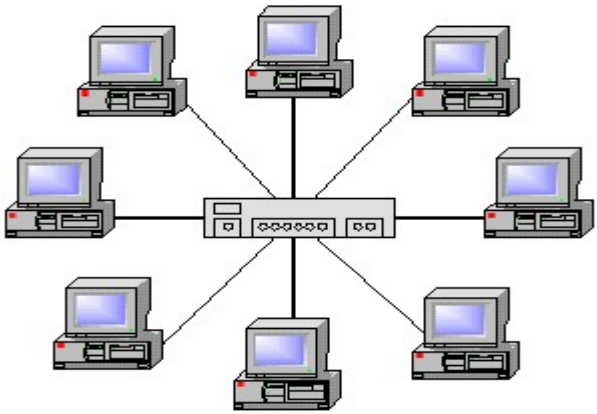

Рис. 10. **Топология "звезда"**

В качестве центрального узла выступает пассивное с точки зрения обработки данных устройство - концентратор (hub), или коммутатор. "Звезда" отличается тем, что не предоставляет возможности двум компьютерам в сети обмениваться данными иначе, чем с помощью посредника - центрального узла.

В сетях с топологией "звезда" подключение кабеля и управление конфигурацией сети централизованы. Так как все компьютеры подключены к центральному узлу отдельными кабелями, для больших сетей значительно увеличивается расход кабеля. К тому же, если центральный узел выйдет из строя, нарушится работа всей сети, однако в данном случае несколько компьютеров в сети могут вести передачу данных одновременно, в то время как шинная топология и топология маркерного кольца в каждый момент времени выделяют только один компьютер, которому позволено передавать данные.

Если выйдет из строя только один компьютер (или кабель, соединяющий его с концентратором), то лишь этот компьютер не сможет передавать или принимать данные по сети. На остальные компьютеры в сети это не повлияет. Для создания звездообразной топологии, в основном, используется кабель "витая пара". В "звезде" центром является концентратор или коммутатор, а лучами - сегменты, на концах которых находятся рабочие станции (по одной на каждый сегмент). В современной сети "звезда" может являться элементом иерархической структуры. Являясь основой для построения структурированных кабельных систем, она отличается относительно высокой стоимостью кабельной системы, позволяет сосредоточить в одном месте все проблемы по передаче данных, по адресации.

Полносвязная топология. Полносвязные топологии соответствуют сети, в которой каждый узел связан со всеми остальными. Несмотря на логическую простоту, это громоздкий и неэффективный вариант. Каждый компьютер такой сети должен содержать огромное количество портов для связи со всеми остальными компьютерами сети. Для каждой пары компьютеров должна быть выделена отдельная линия связи. При этом достигается максимальная производительность, надежность, скорость передачи. Полносвязные топологии в локальных сетях не применяются. Чаще всего этот вид топологии встречается в многомашинных комплексах. Схематично полносвязная топология представлена на рис. 11.

Все другие топологии неполносвязные. Это означает, что для обмена данными между двумя конечными узлами могут потребоваться промежуточные узлы.

Ячеистая, или сотовая, топология. Получается из полносвязной путем удаления некоторых линий связи. Ячеистая топология допускает соединения большого количества компьютеров и характерна для крупных сетей. Применяется в глобальной сети Internet.

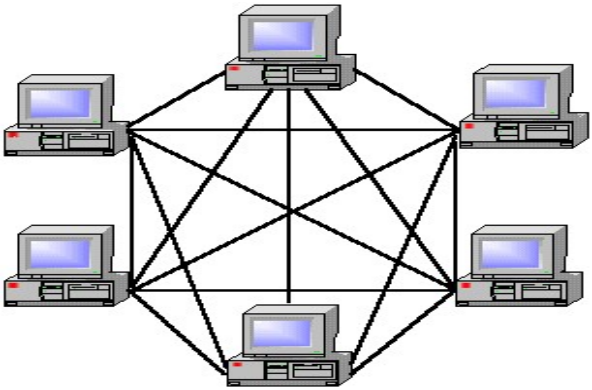

Рис. 11. **Полносвязная топология**

Используется и немалое количество других топологий, которые являются комбинациями уже названных.

Смешанная топология. Большинство более или менее крупных сетей имеют смешанную топологию, в которой можно выделить отдельные фрагменты типовых топологий (см. рис. 9, 10).

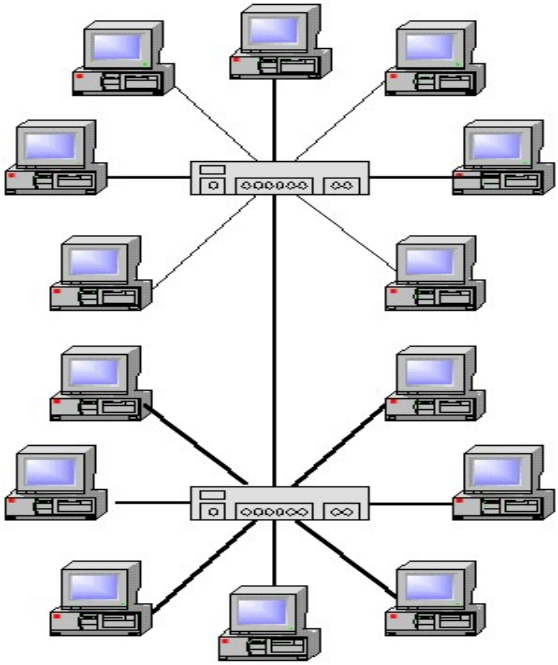

Рис. 12. **Сеть смешанной топологии ("звезда" - "звезда")**

Появление смешанных топологий обусловлено, как правило, необходимостью наращивать и модернизировать сеть. Часто суммарные затраты на постепенную модернизацию оказываются существенно большими, а результаты меньшими, чем при затратах на глобальную замену морально устаревших сетей (рис. 12, 13).

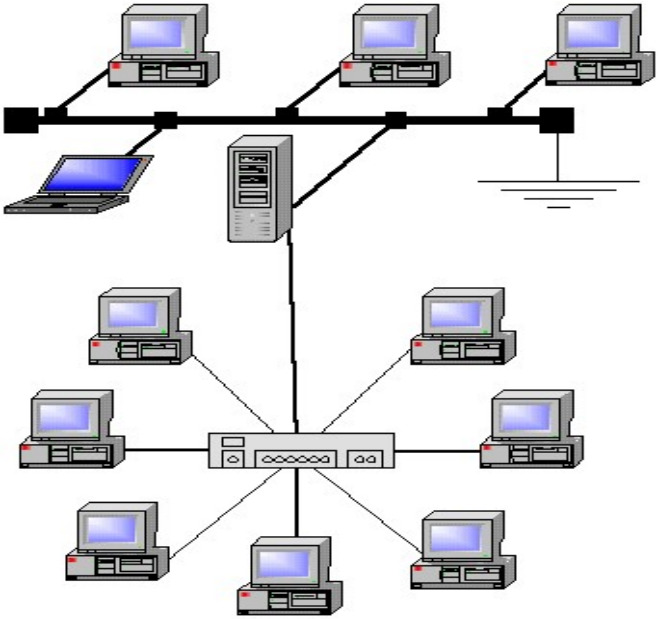

Рис. 13. **Сеть смешанной топологии ("звезда" - "шина")**

Сети смешанной топологии обладают достоинствами и недостатками, характерными для составляющих их топологий.

2.4. Структура IP-адреса, маска сети

Локальные сети с подключением к Internet принято называть TCP/IP, или IP-сетями. Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

1) физический адрес компьютера (аппаратный, адрес канального уровня) - адрес узла, определяемый технологией, с помощью которой построена отдельная локальная сеть, включающая данный узел. Для уз-

лов, входящих в локальные сети, - это MAC-адрес (Medium Accses Controller) сетевого адаптера, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем;

2) IP-адрес, включает 32 двоичных разряда (4 байта) и используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение;

3) символьный идентификатор (символьный, доменный адрес) - имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес называется также DNS-именем. IP-адрес состоит из четырех байтов (октетов) и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например:

- 128.10.2.30 - традиционная десятичная форма представления адреса;
- 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Соотношение между адресом сети и адресом узла зависит от класса IP-адреса. Сейчас определены 5 классов IP-адресов: A, B, C, D, E. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса.

Если адрес начинается с 0, то сеть относят к классу A и номер сети занимает один байт, остальные 3 байта интерпретируются как

номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126 (номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже). В сетях класса А количество узлов должно быть больше 216, но не превышать 224.

Если первые два бита адреса равны 10, то сеть относится к классу В. В сетях класса В под адрес сети и под адрес узла отводится по 16 бит, т.е. по 2 байта.

Если адрес начинается с последовательности 110, то это сеть класса С. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.

Если адрес начинается с последовательности 11110, то это адрес класса Е, он зарезервирован для будущих применений.

На рис. 14 показаны эти пять классов, отличающиеся значениями старшего октета в двоичной системе.

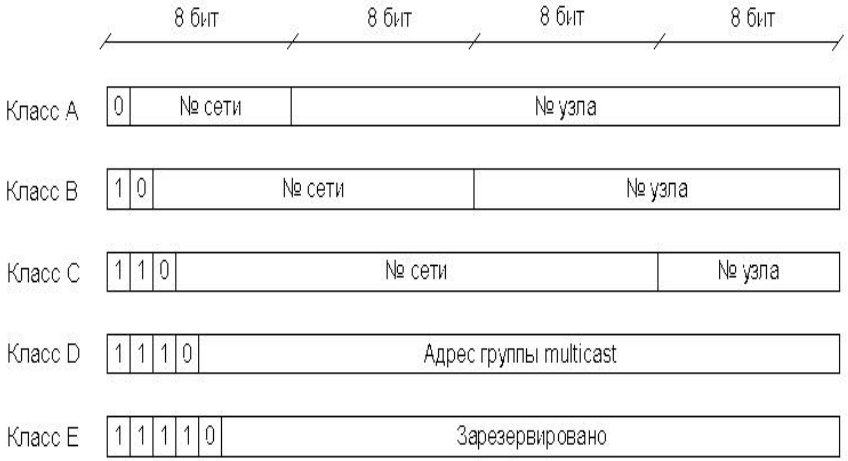

Рис. 14. **Классы IP-адресов в двоичной системе**

Рассмотрим структуру IP-адресов в десятичной системе. Назовем каждую группу чисел в адресе буквами **W.X.Y.Z**. По значению W (первый октет) можно определить, к какому классу относится IP-адрес. В табл. 1 приведена структура IP-адресов в десятичной системе.

Таблица 1

Структура IP-адресов в десятичной системе

Класс	Диапазон значений первого октета	Адрес сети	Адрес узла	Возможное количество сетей	Возможное количество узлов	Маска подсети
A	1 - 126	W	X.Y.Z	126	16 777 214	255.0.0.0
B	128 - 191	W.X	Y.Z	16 382	65 534	255.255.0.0
C	192 - 223	W.X.Y	Z	2 097 150	254	255.255.255.0
D	224 - 239			-	228	
E	240 - 247			-	227	

Для класса A значение W лежит в диапазоне 1 - 126, для класса B значение W принимается от 128 до 191, для класса C - от 192 до 223. Из табл. 1 видно, что возможное количество адресуемых сетей в классе A равно 126, в классах B и C оно возрастает, соответственно, до 16 382 и 2 097 150.

Маска подсети. Она вводится, чтобы в IP-адресе отличить номер сети от номера узла. Маски похожи на IP-адреса, но не несут адресной информации, а лишь говорят о том, какую часть адреса считать адресом подсети, а какую - адресом узла. Например, пусть IP-адрес узла будет 169.234.93.171, а маска подсети 255.255.0.0. Если представить адрес и маску в двоичном виде, то адресом подсети будет та часть адреса, которой соответствуют единицы в записи маски, а адресом узла - та часть, которая содержит нули. В табл. 2 приведены IP-адрес и маска подсети.

Таблица 2

IP-адрес и маска подсети

IP-адрес в десятичной записи	IP-адрес в двоичной записи
169.234.93.171	10101001.11101010.01011101.10101011
Маска подсети 255.255.0.0	11111111.11111111.00000000.00000000

Эта информация используется при настройке сети. В случае с локальной сетью многие настройки делаются автоматически, но пользователь должен знать возможность их ручной модификации.

Соглашения о специальных адресах: broadcast, multicast, loopback . В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

• если IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;

- если в поле номера сети стоит 0, то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет;
- если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);
- если в поле адреса сети назначения стоят сплошные 1, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast);
- адрес **127.0.0.1** зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

Форма группового IP-адреса multicast означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, т.е. определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Такие сообщения, в отличие от широковещательных, называются мультивещательными. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

В протоколе IP нет понятия широковещательности в том смысле, в котором оно используется в протоколах канального уровня локальных сетей, когда данные должны быть доставлены абсолютно всем узлам. Как ограниченный широковещательный IP-адрес, так и широковещательный IP-адрес имеют пределы распространения в интерсети - они ограничены либо сетью, к которой принадлежит узел - источник пакета, либо сетью, номер которой указан в адресе назначения. Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из составляющих общую сеть частей.

"Белые" и "серые" IP-адреса. "Белыми" называют IP-адреса, которые видны (доступны) из Internet. Например, адрес 89.186.236.4 доступен из Internet, он присвоен службе DNS сети СГЭУ. А IP-адреса компьютеров, подключенных в Internet через локальную сеть, являются "серыми". Выделены специальные сетки "серых" IP-адресов локальных сетей для разных классов: для класса A - 10.0.0.0; для класса B - 10.10.0.0, 172.16.0.0 - 172.31.0.0; для класса C - 10.10.10.0, 192.168.0.0 - 192.168.254.0.

Введение "серых" IP-адресов позволило увеличить количество IP-адресов в Internet, иначе 32-разрядного цифрового адреса не хватило бы для подключения к Internet такого количества пользователей. Подключение компьютеров с "серыми" IP-адресами к Internet выполняется через специальные службы или устройства. Это может быть прокси-сервер или маршрутизатор (роутер), обладающие функцией трансляции адресов (NAT), которые заменяют своим "белым" IP-адресом "серые" адреса, запоминая их специальным образом.

Для определения адреса сети в конкретном IP-адресе используется маска подсети. Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.0.0 находится в сети 12.34.0.0.

Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И). Например, в случае более сложной маски:

IP-адрес: 00001100 00100010 00111000 01001110 (12.34.56.78);

маска подсети: 11111111 11111111 11100000 00000000 (256.256.224.0);

адрес сети: 00001100 00100010 00100000 00000000 (12.34.32.0).

Маску подсети часто записывают вместе с IP-адресом в формате ***IP-адрес/количество единичных бит в маске***. Например, IP-адрес 12.34.56.78 с маской 255.255.224.0 (т.е. состоящей из 19 единичных бит и 13 нулевых) можно записать как 12.34.56.78/19.

Разбиение одной большой сети на несколько маленьких подсетей позволяет упростить маршрутизацию. Например, пусть таблица маршрутизации некоего маршрутизатора содержит следующую запись (табл. 3):

Таблица 3

Таблица маршрутизации

Сеть назначения	Маска	Адрес шлюза
12.34.0.0	255.255.0.0	11.22.3.4

Пусть теперь маршрутизатор получает пакет данных с адресом назначения 12.34.56.78. Обрабатывая построчно таблицу маршрутизации, он обнаруживает, что при наложении маски 255.255.0.0 на адрес 12.34.56.78 получается адрес сети 12.34.0.0. В таблице маршрутизации этой сети соответствует шлюз 11.22.3.4, которому и отправляется пакет.

Маски подсети являются основой метода ***бесклассовой маршрутизации***.

Маска назначается по следующей схеме $2^8 - n$ (для сетей класса C), где n - количество компьютеров в подсети + 2, округленное до ближайшей большей степени двойки.

Пример: в сети класса С есть 30 компьютеров, маска для такой сети вычисляется следующим образом:

$$2^8 - 30 + 2 = 256 - 32 = 224.$$

Маска выглядит так: 255.255.255.224.

В настоящее время обсуждается вопрос об увеличении разрядности IP-адреса до 128, поскольку уже возник дефицит IP-адресов. Уже в 1996 г. было зарегистрировано более 100 000 сетей. Разбивка сетей на три класса А, В и С уже не может отвечать современным требованиям. Сеть класса А с ее 17 000 000 адресов слишком велика, а класса С с 254 адресами, как правило, слишком мала. Сети класса В с 65 536 машинами могут показаться оптимальными, но на практике каждая из этих сетей не обеспечивает оптимального использования адресного пространства и всегда остаются неиспользованные адреса (для классов В и А количество пустующих адресов оказывается обычно значительным).

Если бы в адресах класса С для кода номера ПК было выделено 10 или 11 бит (1024-2048), ситуация была бы более приемлемой. Маршрутизатор рассматривает IP-адресную среду на двух уровнях - адрес сети и адрес ЭВМ, при этом практически они работают только с адресами сетей. Число записей в маршрутной таблице должно будет быть равным половине миллиона записей (по числу блоков С-адресов).

Проблема может быть решена, если забыть про разбиение всей совокупности IP-адресов на классы. Бесклассовая адресация (Classless Inter Domain Routing, CIDR) - метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жесткие рамки классовой адресации. Применение этого метода позволяет экономно использовать конечный ресурс IP-адресов.

Бесклассовая адресация основывается на переменной длине маски подсети (Variable Length Subnet Mask - VLSM), в то время как в классовой адресации длина маски строго фиксирована 1, 2 или 3 установленными байтами. Вот пример записи IP-адреса с применением бесклассовой адресации: 10.1.2.33/27 (табл. 4).

Таблица 4

Пример записи IP-адреса с применением бесклассовой адресации

Октеты IP-адреса	10	1	2	33
Биты IP-адреса	00001010	00000001	00000010	00100001
Биты маски подсети	11111111	11111111	11111111	11100000
Октеты маски подсети	255	255	255	224

В данном примере видно, что в маске подсети 27 бит слева выставлены в единицу (так называемые значащие биты). В таком случае говорят о длине маски подсети в 27 бит (/27 - на сленге "слэш двадцать семь").

Таблица 5

Пример записи IP-адреса с применением бесклассовой адресации

Октеты IP-адреса	172								16								0								1							
Биты IP-адреса	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Биты маски подсети	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Октеты маски подсети	255								240								0								0							

Еще один пример записи адреса 172.16.0.1/12 в бесклассовой системе адресации приведен в табл. 5.

2.5. Концепции адресации в сетях

Наука об объединении сетей, как и другие науки, имеет свою собственную терминологию и научную базу. К сожалению, ввиду того, что эта наука очень молода, пока что не достигнуто единое соглашение о значении концепций и терминов объединенных сетей. По мере дальнейшего совершенствования индустрии объединенных сетей определение и использование терминов будут более четкими.

Значимый компонент любой системы сети - определение местонахождения компьютерных систем. Существуют различные схемы адресации, используемые для этой цели, которые зависят от используемого семейства протоколов. Двумя важными типами адресов являются адреса канального уровня и адреса сетевого уровня. Адреса канального уровня (называемые также физическими, или аппаратными, адресами), как правило, уникальны для каждого сетевого соединения. У большинства локальных сетей адреса канального уровня размещены в схеме интерфейса (в сетевом адаптере), они назначаются той организацией, которая определяет стандарт протокола, представленный этим интерфейсом. Так как большинство компьютерных систем имеют одно физическое сетевое соединение, у них только один адрес канального уровня. Маршрутизаторы и другие системы, соединенные с множеством физических сетей, могут иметь множество адресов канального уровня. В соответствии с названием адреса канального уровня существуют на втором уровне эталонной модели ISO.

Адреса сетевого уровня (называемые также виртуальными, или логическими, адресами) существуют на третьем уровне эталонной модели OSI. В отличие от адресов канального уровня, которые обычно находятся в пределах плоского адресного пространства, адреса сетевого уровня обычно иерархические. Другими словами, они похожи на почтовые адреса, которые описывают местонахождение человека, указывая страну, штат, почтовый индекс, город, улицу, адрес на этой улице и имя.

Иерархические адреса делают сортировку адресов и повторный вызов более легким путем исключения крупных блоков логически схожих адресов в процессе последовательности операций сравнения. Например, можно исключить все другие страны, если в адресе указана страна. Легкость сортировки и повторного вызова является причиной того, что маршрутизаторы (роутеры) используют адреса сетевого уровня в качестве базиса маршрутизации.

2.6. Понятие протоколов вычислительных сетей

Понятие протокола, вытекающее из эталонной модели OSI, - это набор правил, определяющий взаимодействие двух одноименных уровней модели взаимодействия открытых систем в различных сетевых ЭВМ. Функции протоколов различных уровней реализуются в драйверах для различных вычислительных сетей.

Современные сети построены по многоуровневому принципу. Чтобы организовать связь двух компьютеров, требуется сначала определить свод правил их взаимодействия, определить язык их общения и то, что означают посылаемые ими сигналы, и т.д. Эти правила и определения называются протоколами.

Протокол можно также рассматривать как совокупность определений (соглашений, правил), регламентирующих формат и процедуры обмена информацией между двумя или несколькими независимыми устройствами или процессами, т.е. как описание того, как программы, компьютеры или иные устройства должны работать, когда они взаимодействуют друг с другом.

Протокольные определения охватывают диапазон от того, в каком порядке биты следуют по проводу, до формата сообщения элек-

тронной почты. Стандартные протоколы позволяют связываться друг с другом компьютерам различных производителей. Взаимодействующие компьютеры могут использовать различное программное обеспечение, но должны соблюдать принятое соглашение о том, как посылать и принимать данные.

Для работы сетей необходимо множество различных протоколов: например, управляющих физической связью, установлением связи по сети, доступом к различным ресурсам и т.д. Многоуровневая структура используется с целью упростить это огромное множество протоколов и отношений. Она позволяет также составлять сетевые системы из продуктов - модулей программного обеспечения, - выпущенных разными производителями.

2.7. Стеки протоколов

Набор протоколов, работающих одновременно и совместно в одной сети, называется стеком (stack) протоколов. Рассмотрим основные стеки, используемые в разных сетях.

Стек TCP/IP. Самым известным стеком протоколов является стек TCP/IP (Transfer Communication Protocol/Internet Protocol), который ведет свою историю от сети ARPAnet. Он получил свое название от пары протоколов: протокола IP сетевого уровня, который обеспечивает доставку данных между узлами, и протокола TCP транспортного уровня, который делает эту доставку надежной. Помимо этих протоколов, стек TCP/IP включает и множество других. С TCP/IP работают десятки миллионов компьютеров во всем мире, на его основе действуют все больше внутренних сетей фирм, предприятий (Intranet).

Стек IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange). Это фирменная разработка компании Novell. Стек IPX/SPX разрабатывался для сетевой операционной системы Novell Netware в 80-х гг. XX в. и сегодня не утратил популярности. Поддержка этого стека, как и стека TCP/IP, встроена в Windows XP. IPX - протокол сетевого уровня модели OSI, на транспортном уровне работает протокол SPX.

Преимущество IPX/SPX заключалось в том, что он был ориентирован на работу с довольно слабыми ПК в локальных сетях с исполь-

зованием широковещательной рассылки пакетов. В TCP/IP это недопустимо, здесь осуществляется маршрутизация пакетов по указанному адресу. Стек IPX/SPX продолжает развиваться, но по популярности давно уступает стеку TCP/IP.

Стек NETBIOS. Стек NetBIOS (Network Input/Otput/ System) разработан как сетевое расширение BIOS и предназначен для работы в простых локальных сетях. Он состоит из протоколов NetBIOS и SMB (Server Message Block). Современная реализация NETBIOS называется NetBEUI и используется в сетях Microsoft.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня - физический, канальный и сетевой - являются сетезависимыми, т.е. протоколы этих уровней тесно связаны с технической реализацией сети, с используемым коммуникационным оборудованием. Например, переход на оборудование FDDI означает полную смену протоколов физического и канального уровней во всех узлах сети.

Три верхних уровня - сеансовый, уровень представления и прикладной - ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют никакие изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних уровней. Это позволяет разрабатывать приложения, не зависящие от технических средств, непосредственно занимающихся транспортировкой сообщений.

Компьютер с установленной на нем сетевой операционной системой взаимодействует с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство может работать либо только на физическом уровне (повторитель), либо на физическом и канальном (мост), либо на физическом, канальном и сетевом, иногда захватывая и более высокие уровни (маршрутизатор).

Модель OSI представляет хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, сервисами, предоставляемыми на верхних уровнях, и прочими параметрами.

2.8. Доменная система имен

Рассмотрим подробнее доменную систему имен, применяемую в Internet. Система доменных имен DNS (Domain Name System) строится по иерархическому принципу. Однако эта иерархия не строгая. Фактически нет единого корня для всех доменов Internet. Если быть точным, то такой корень в модели DNS есть, он называется ROOT. Но единого администрирования этого корня нет. Администрирование в Internet начинается с доменов верхнего (первого) уровня.

В системе доменов верхнего уровня в Internet приняты домены, представленные географическими (национальными) регионами. Они имеют имя, состоящее из двух букв. Например, географические домены для некоторых стран: Франция - fr; США - us; Россия - ru.

Существуют и домены, поименованные по тематическим признакам, они имеют трехбуквенное обозначение. Например, коммерческие организации - com; правительственные учреждения - gov, сервисные центры, Internet, американские университеты - edu, военные сети США - mil.

Данная система обозначений пошла из США. В 1980-е гг. там, на родине Internet, были определены первые домены верхнего уровня, и это были трехбуквенные обозначения. Затем, когда сеть перешагнула границы США, появились национальные домены (двухбуквенные), для СССР был выделен домен su, далее, когда в конце 80-х республики Советского Союза стали самостоятельными, России дали домен ru. Но выбросить домен su из употребления уже нельзя, поскольку на основе доменных имен строятся адреса электронной почты и доступ ко многим ресурсам Internet. Поэтому в России сейчас есть организации с доменными именами ru, рф и su. **DNS (Domain Name System)** - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами **RFC 1034 и 1035**. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet.

Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет, то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром **Internet Network Information Center.** Домены верхнего уровня назначаются для каждой страны. Имена этих доменов должны следовать международному стандарту ISO 3167. Для обозначения стран используются двухбуквенные аббревиатуры (уже упоминалось выше), а для различных типов организаций используются следующие аббревиатуры:

- com - коммерческие организации (например, microsoft.com);
- edu - образовательные (например, mit.edu);
- gov - правительственные организации (например, nsf.gov);
- org - некоммерческие организации (например, fidonet.org);
- net - коммерческие сети или узлы Internet (например, nsf.net);
- biz - организации, занимающиеся бизнесом;
- info - информационные сайты.

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно опре-

деляется своим полным доменным именем (fully qualified domain name, FQDN), которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени: citint.dol.ru. Корневой домен Internet управляется несколькими организациями, в частности Network Solutions, Inc.

Сервис DNS строится по схеме клиент-сервер. В качестве клиентской части выступает процедура разрешения имен - resolver, а в качестве сервера - DNS-сервер (пакет BIND, являющийся де-факто стандартом DNS-сервера).

Дерево доменных имен аналогично файловой системе Unix. Корнем дерева является домен "." (точка). Полное - абсолютное или полностью определенное - имя FQDN заканчивается точкой, обозначающей корень доменного дерева, но часто эта завершающая точка опускается. Доменами верхнего (первого) уровня выступают двухбуквенные национальные домены или трехбуквенные домены com, edu, org, net, gov, int, mil (рис. 15).

Рис. 15. **Структура службы доменных имен**

На приведенной схеме верхний (первый) уровень обозначен **I**, второй уровень - **II**. Каждому объекту трех верхних уровней соответствуют серверы имен, которые могут взаимодействовать друг с другом при решении задачи преобразования имени в IP-адрес. Каждый сервер содержит лишь часть дерева имен. Эта часть называется зоной ответственности сервера. DNS-сервер может делегировать ответственность за часть зоны другим серверам, создавая субзоны. Когда в зоне появляется новая ЭВМ или субдомен, администратор зоны запи-

сывает ее имя и IP-адреса в базу данных сервера. Администратор зоны определяет, какой из DNS-серверов имен является для данной зоны первичным. Число вторичных серверов не лимитировано. Первичный и вторичный серверы должны быть независимыми и работать на разных ЭВМ так, чтобы отказ одного из серверов не выводил из строя систему в целом. Отличие первичного сервера имен от вторичного заключается в том, что первичный загружает информацию о зоне из файлов на диске, а вторичный получает ее от первичного сервера. Администратор вносит любые изменения в соответствующие файлы первичного сервера, а вторичные серверы получают эту информацию, периодически запрашивая первичный сервер. Пересылка информации из первичного во вторичные серверы имен называется зонным обменом.

Список корневых серверов можно получить по протоколу FTP по адресам: **nic.ddn.mil** или **ftp.rs.internic.net**.

Серверы первого уровня хранят информацию об именах и адресах всех серверов доменов второго уровня.

Преобразования "доменное имя в IP-адрес" ("прямое") выполняются службой DNS путем поиска в доменном дереве нужного имени и извлечения связанной с этим именем информации требуемого типа (IP-адрес). Существует также обратное DNS-преобразование "IP-адрес в доменное имя".

Программа (утилита) NSLOOKUP. Программа позволяет произвести DNS-преобразования в явном виде. Служит для диагностики DNS-серверов. Может использоваться из командной строки в формате NSLOOKUP. Например, просмотрим все серверы имен домена microsoft.com. Вводим через команду ПУСК - ВЫПОЛНИТЬ - cmd команду: nslookup/type=ns microsoft.com.

Результат выполнения команды:

```
Server: msuvx1.memphis.edu
Address: 141.225.1.2
Non-authoritative answer:
MICROSOFT.COM NAMESERVER = DNS3.NWNET.NET
MICROSOFT.COM NAMESERVER = DNS4.NWNET.NET
MICROSOFT.COM NAMESERVER = ATBD.MICROSOFT.COM
MICROSOFT.COM NAMESERVER = DNS1.MICROSOFT.COM
DNS3.NWNET.NET INTERNET ADDRESS = 192.220.250.7
DNS4.NWNET.NET INTERNET ADDRESS = 192.220.251.7
ATBD.MICROSOFT.COM INTERNET ADDRESS = 131.107.1.7
DNS1.MICROSOFT.COM INTERNET ADDRESS = 131.107.1.7
```

DNS1.MICROSOFT.COM INTERNET ADDRESS = 131.107.1.240

В данном примере использован ключ -type=ns, так как был необходим лишь список DNS-серверов. Выданы имена серверов доменных имен и их IP-адреса.

Утилита может использоваться в интерактивном режиме, перенаправляя запросы другим серверам. Для получения информации о параметрах утилиты следует ввести ее имя со знаком "?": **nslookup /?**

2.9. Схемы адресации ресурсов Internet

В стандарте RFC-1630 рассмотрены схемы адресации ресурсов Internet. Далее представлены некоторые наиболее популярные ресурсы.

Схема HTTP (Hyper Text Transfer Protocol). Это основная схема (протокол) для WWW-технологий. Серверы, работающие на языке протокола HTTP, называются HTTP-серверами, или WEB-серверами.

Нами уже рассмотрен пример адресации ресурса по протоколу HTTP. Напомним, что такой адрес может заканчиваться символами метки (как было рассмотрено) или символом поиска ресурса по ключевым словам. При передаче ключевых слов употребляется служебный символ "?" в таком виде:

http://paul.net.kiae.su/kadr.html?keyword1.

В данном примере предполагается, что данный документ kadr.html - это документ с возможностью поиска по ключевым словам (после вопросительного знака дано ключевое слово *keyword1*). Чаще всего указывается только имя ресурса без меток и ключевых слов. Если имя файла неизвестно, можно обратиться к соответствующему серверу, получить на экран его исходную страницу и воспользоваться подсказками для поиска нужной информации. Как правило, исходные страницы WEB-серверов обязательно содержат понятные подсказки в виде красочных меню.

Схема FTP. Эта схема также позволяет адресовать файловые архивы FTP из программ-клиентов WWW (броузеров). Известно, что доступ к архивам FTP может быть анонимным (неавторизованный доступ) и авторизованным, когда надо указывать идентификатор пользователя и даже его пароль. Неавторизованный доступ возможен только к публичным, некоммерческим архивам. В связи с этим существует два варианта адресации:

Неавторизованный доступ: ftp://polyn.net.kiae.su/pub/1index.txt.

В данном случае записана ссылка на ресурс с подразумеваемым идентификатором "anonymous". Это пример обращения к публичному архиву. В Internet много публичных ftp-серверов. Список таких серверов можно взять на ftp-сервере garbo.uwasa.fi.

Авторизованный доступ: *ftp://nobody1:password@polyn.net.kiae.su/users/local/pub.*

В данном случае идентификатор (nobody1) и пароль (password) отделены от адреса машины символом "@". По введенной команде указанный файл будет (в случае успешного обнаружения) передан на ваш компьютер. Если вы не знаете точное имя ресурса, но вам известно имя ftp-сервера, на котором он расположен, можно обратиться к исходной странице этого сервера, а затем с нее попытаться найти соответствующий файл и дать команду на его перекачку на ваш компьютер.

TELNET. По данной схеме осуществляется доступ к ресурсу в режиме удаленного терминала. При использовании этой схемы обычно применяется пароль. Пример: telnet://guest:password@apollo.polyn.kiae.su.

По этой команде ваш компьютер окажется терминалом компьютера с указанным доменным именем, и можно просматривать то, что вам разрешено, и в той системе, которая работает на этом компьютере.

2.10. Сетевая модель Internet и стек протоколов TCP/IP

Стек TCP/IP был разработан по инициативе министерства обороны США более 20 лет назад для связи экспериментальной сети ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Большой вклад в развитие стека TCP/IP, который получил свое название по популярным протоколам IP и TCP, внес университет Беркли, реализовав протоколы стека в своей версии ОС UNIX. Популярность этой операционной системы привела к широкому распространению протоколов TCP, IP и других протоколов стека. Сегодня этот стек используется для связи компьютеров всемирной информационной сети Internet, а также в огромном числе корпоративных сетей.

Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней: для локальных сетей -

это Ethernet, Token Ring, FDDI; для глобальных - протоколы работы на аналоговых коммутируемых и выделенных линиях SLIP, PPP, протоколы территориальных сетей X.25.

TCP/IP - собирательное название для набора (стека) сетевых протоколов разных уровней в сети Internet. За долгие годы применения в сетях различных стран и организаций стек TCP/IP вобрал в себя большое количество протоколов прикладного уровня. К ним относятся такие популярные протоколы, как протокол пересылки файлов FTP, почтовый протокол SMTP, используемый в электронной почте сети Ethernet, гипертекстовые сервисы службы WWW и многие другие. Сеть Internet - это сеть сетей, объединяющая как локальные, так и глобальные сети. Поэтому центральным местом при обсуждении принципов построения сети является семейство протоколов межсетевого обмена TCP/IP.

Особенности TCP/IP:

- открытые стандарты протоколов, разрабатываемые независимо от программного и аппаратного обеспечения;
- независимость от физической среды передачи;
- система уникальной адресации;
- стандартизованные протоколы высокого уровня для распространенных пользовательских сервисов.

Сетевая модель Internet (рис. 16) представлена четырьмя уровнями. На рисунке приведены также основные протоколы стека TCP/IP.

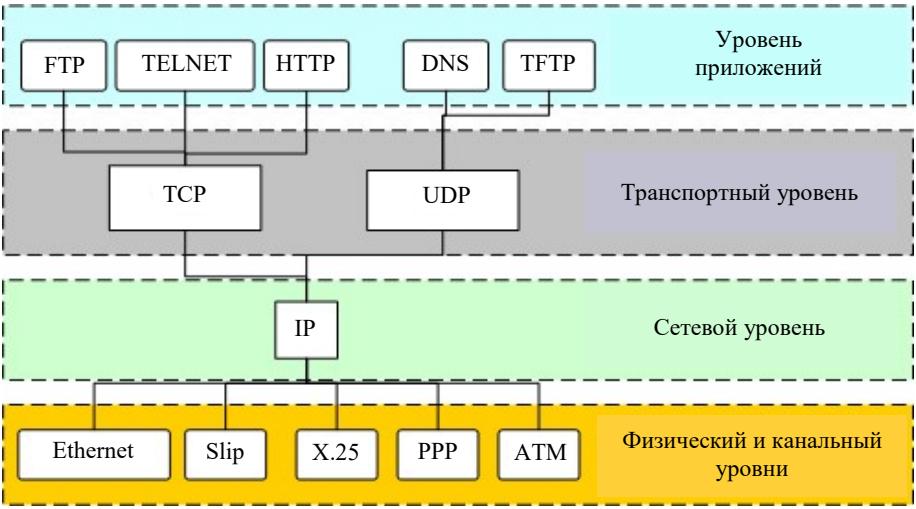

Рис. 16. **Сетевая модель Internet**

Стек протоколов TCP/IP делится на 4 уровня:

- прикладной (уровень приложений);
- транспортный;
- сетевой (межсетевой);
- физический и канальный, называемый также *уровнем доступа к сети*.

Данные передаются в пакетах. Данные верхних уровней вставляются в пакеты нижних уровней. Инкапсуляция - способ упаковки данных в формате одного протокола в формат другого протокола. Например, упаковка IP-пакета в кадр Ethernet или TCP-сегмента в IP-пакет. Согласно словарю иностранных слов термин "инкапсуляция" означает "образование капсулы вокруг чужих для организма веществ (инородных тел, паразитов и т.д.)". В рамках межсетевого обмена понятие инкапсуляции имеет несколько более расширенный смысл. Если в случае инкапсуляции IP в Ethernet речь идет действительно о помещении пакета IP в качестве данных Ethernet-кадра или в случае инкапсуляции TCP в IP помещение TCP-сегмента в качестве данных в IP-пакет, то при передаче данных по коммутируемым каналам происходит дальнейшая "нарезка" пакетов теперь уже на пакеты SLIP или фреймы PPP. Пример инкапсуляции пакетов в стеке TCP/IP приведен на рис. 17.

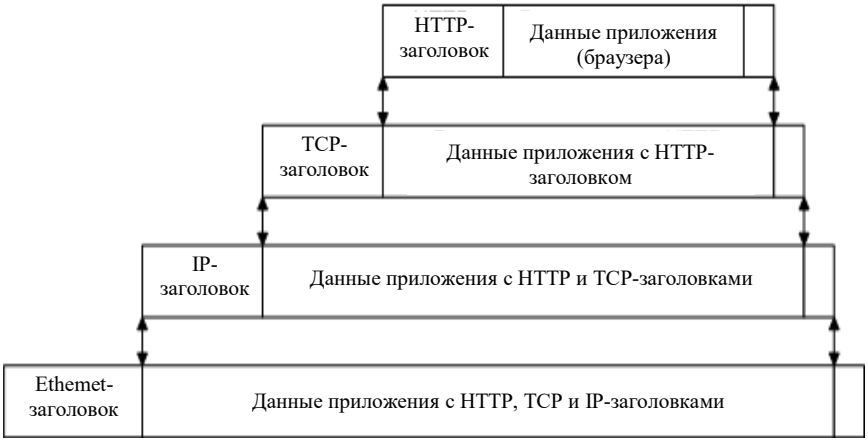

Рис. 17. **Пример инкапсуляции пакетов в стеке TCP/IP**

Главной задачей стека TCP/IP является объединение в сеть пакетных подсетей через шлюзы. Каждая сеть работает по своим собственным законам, однако предполагается, что шлюз может принять

пакет из другой сети и доставить его по указанному адресу. Пакет из одной сети передается в другую подсеть через последовательность шлюзов, которые обеспечивают сквозную маршрутизацию пакетов по всей сети. В данном случае под шлюзом понимается точка соединения сетей. При этом соединяться могут как локальные, так и глобальные сети. В качестве шлюза могут выступать как специальные устройства, маршрутизаторы, так и компьютеры, которые имеют программное обеспечение, выполняющее функции маршрутизации пакетов. Маршрутизация - это процедура определения пути следования пакета из одной сети в другую. На рис. 18 представлена схема объединения сетей.

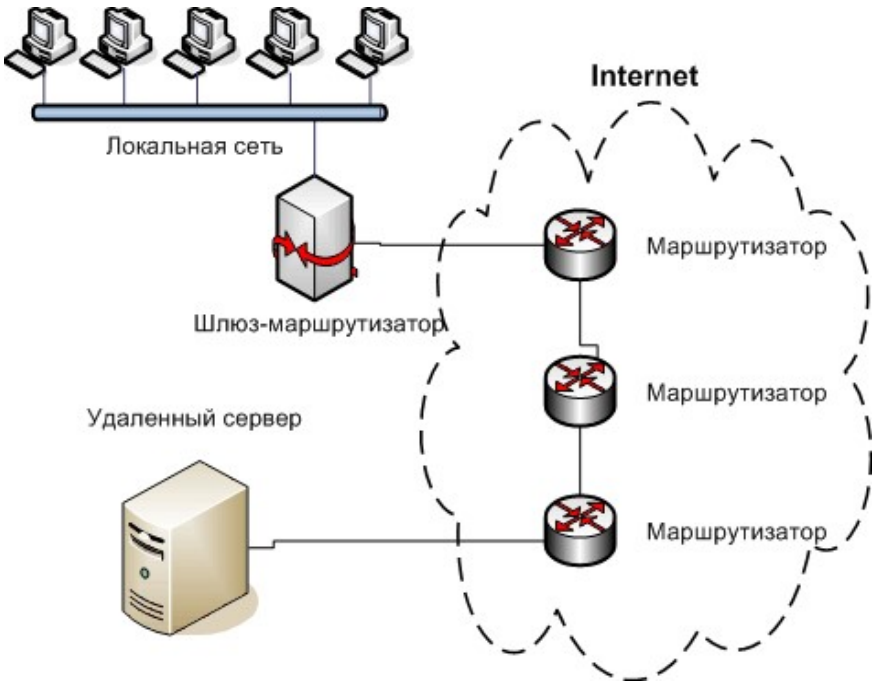

Рис. 18. **Схема объединения ЛВС и Internet**

Сегодня стек TCP/IP представляет собой один из самых распространенных стеков протоколов вычислительных сетей. Только в сети Internet объединено более 10 миллионов компьютеров по всему миру, которые взаимодействуют друг с другом с помощью стека протоколов TCP/IP. Рассмотрим основные протоколы всех уровней сетевой модели Internet.

2.11. Уровень доступа к сети

К этому уровню отнесены протоколы, определяющие соединение с Internet, например, **SLIP (Serial Line Internet Protocol)** - протокол передачи данных по телефонным линиям; PPP (Point to Point Protocol) - протокол соединения "точка-точка"; протоколы Ethernet IEEE 802.03, Token Ring, ATM и др.

SLIP (Serial Line Internet Protocol). Это устаревший сетевой протокол канального уровня эталонной сетевой модели OSI для доступа к сетям стека TCP/IP через низкоскоростные линии связи путем простой инкапсуляции IP-пакетов. Используются коммутируемые соединения через последовательные порты для соединений клиент-сервер типа "точка-точка". В настоящее время вместо него используют более совершенный протокол PPP.

PPP (Point-to-Point Protocol). Это протокол "точка-точка" - механизм для создания и запуска IP и других сетевых протоколов на последовательных линиях связи. Протокол PPP является основой для всех протоколов канального уровня. Связь по протоколу PPP состоит из четырех стадий: установление связи (осуществляется выбор протоколов аутентификации, шифрования, сжатия, и определяются параметры соединения); установление подлинности пользователя; контроль повторного вызова PPP (необязательная стадия, в которой подтверждается подлинность удаленного клиента); вызов протокола сетевого уровня. Обычно используется для установки прямых соединений между двумя узлами. Широко применяется для соединения компьютеров с помощью телефонной линии. Также используется поверх широкополосных соединений. Многие Internet-провайдеры используют PPP для предоставления коммутируемого доступа в Internet.

2.12. Сетевой уровень модели Internet

К сетевому уровню относятся протоколы, которые отвечают за отправку и получение данных, или, другими словами, за соединение отправителя и получателя.

Протокол IP. Является самым главным во всей иерархии протоколов семейства TCP/IP. Именно он используется для управления рассылкой TCP/IP-пакетов по сети Internet. Важнейшие функции протокола IP:

- определение пакета, который является базовым понятием и единицей передачи данных в сети Internet (многие зарубежные авторы называют такой IP-пакет датаграммой);
- определение адресной схемы, которая используется в сети Internet;
- передача данных между канальным уровнем (уровнем доступа к сети) и транспортным уровнем;
- маршрутизация пакетов по сети, т.е. передача пакетов от одного шлюза к другому с целью передачи пакета узлу-получателю;
- "нарезка" и сборка из фрагментов пакетов транспортного уровня.

Главными особенностями протокола IP является отсутствие ориентации на физическое или виртуальное соединение. Это значит, что, прежде чем послать пакет в сеть, модуль операционной системы, реализующий IP, не проверяет возможность установки соединения, т.е. никакой управляющей информации, кроме той, что содержится в самом IP-пакете, по сети не передается. Кроме этого, IP не заботится о проверке целостности информации в поле данных пакета, что заставляет отнести его к протоколам ненадежной доставки. Целостность данных проверяется протоколами транспортного уровня (TCP) или протоколами приложений.

Таким образом, вся информация о пути следования пакета формируется в самой сети в момент его прохождения. Именно эта процедура и называется маршрутизацией в отличие от коммутации, использующейся для предварительного установления маршрута следования данных, по которому потом эти данные отправляют.

Принцип маршрутизации является одним из тех факторов, который обеспечил гибкость сети Internet и ее преимущество в сравнении с другими сетевыми технологиями. К сетевому уровню относят также протоколы, выполняющие вспомогательные функции по отношению к IP. Это прежде всего протоколы маршрутизации RIP и OSPF, занимающиеся изучением топологии сети, определением маршрутов и составлением таблиц маршрутизации, на основании которых протокол IP перемещает пакеты в нужном направлении. Также к сетевому уровню относятся еще два протокола.

ICMP (Internet Control Message Protocol). Протокол применяется для рассылки информационных и управляющих сообщений. При этом используются следующие виды сообщений:

- *Flow control* - если принимающий узел (шлюз или реальный получатель информации) не успевает перерабатывать информацию, то данное сообщение приостанавливает отправку пакетов по сети;
- *Detecting unreachable destination* - если пакет не может достичь места назначения, то шлюз, который не может доставить пакет, сообщает об этом отправителю пакета. Информировать о невозможности доставки сообщения может и машина, чей IP-адрес указан в пакете. Только в этом случае речь будет идти о портах TCP и UDP, о чем будет сказано чуть позже;
- *Redirect routing* - это сообщение посылается в том случае, если шлюз не может доставить пакет, но у него есть на этот счет некоторые соображения, а именно адрес другого шлюза;
- *Checking remote host* - в этом случае используется так называемое ICMP Echo Message. Если необходимо проверить наличие стека TCP/IP на удаленной машине, то на нее посылается сообщение этого типа. Как только система получит это сообщение, она немедленно подтвердит его получение.

IGMP (Internet Group Management Protocol). Это протокол групповой рассылки, направляющий пакеты сразу по нескольким адресам.

Развитие протокола IP. Протокол IPv6 (Internet Protocol version 6) - это новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при ее использовании в Internet. В настоящее время протокол IPv6 уже применяется в нескольких сотнях сетей по всему миру, но пока еще не получил широкого распространения в Internet, где преимущественно встречается IPv4. Протокол был разработан организацией **IETF.**

Протокол IP в настоящее время столкнулся с рядом проблем, таких как масштабируемость сети, неприспособленность протокола к передаче мультисервисной информации с поддержкой различных классов обслуживания, включая обеспечение информационной безопасности. Указанные проблемы обусловили развитие классической версии протокола IPv4 в направлении разработки версии IPv6. При этом к проблемам масштабируемости протокола IPv4 следует отнести следующие:

- недостаточность объема 32-битного адресного пространства;
- сложность агрегирования маршрутов, разрастание таблиц маршрутизации;
- сложность массового изменения IP-адресов;
- относительная сложность обработки заголовков пакетов IPv4.

Кроме того, масштабируемость IP-сетей следует рассматривать не только с точки зрения увеличения числа узлов, но и с точки зрения повышения скорости передачи и уменьшения задержек при маршрутизации.

В данной связи было разработано множество версий протокола IP для различных вычислительных платформ и операционных систем. До недавнего времени существовало несколько альтернативных вариантов протокола IP нового поколения. В июле 1994 г. была принята версия протокола нового поколения, получившего название IPv6. В технической литературе эту версию протокола еще называют IPng (IP next generation), хотя иногда под IPng понимают все варианты модернизации IP, включая также не вошедшие в проект IPv6, но продолжающие развиваться. Документом, фиксирующим появление IPv6, является спецификация RFC 1752 "The Recommendation for the IP Next Generation Protocol". Базовый набор протоколов IPv6 был принят IETF в сентябре 1995 г. и получил статус Proposed Standard.

В спецификации RFC 1726 представлен набор функций, основными среди них являются:

- масштабируемость: идентификация и определение адресов как минимум 10^{12} конечных систем и 10^9 индивидуальных сетей;
- топологическая гибкость: архитектура маршрутизации и протокол должны работать в сетях с различной топологией;
- преемственность: обеспечение четкого плана перехода от существующей версии IPv4;
- независимость от среды передачи: работа среди множества сетей с различными средами передачи данных со скоростями до сотен гигабит в секунду;
- автоматическое конфигурирование хостов и маршрутизаторов;
- безопасность на сетевом уровне;
- мобильность: обеспечение работы с мобильными пользователями, сетями и межсетевыми системами;
- расширяемость: возможность дальнейшего развития в соответствии с новыми потребностями.

В результате реализации заявленных функций важнейшие инновации IPv6 состоят в следующем:

- упрощен стандартный заголовок IP-пакета;
- изменено представление необязательных полей заголовка;
- расширено адресное пространство;
- улучшена поддержка иерархической адресации, агрегирования маршрутов и автоматического конфигурирования адресов;

• введены механизмы аутентификации и шифрования на уровне IP-пакетов;

• введены метки потоков данных.

При этом в IPv6 все изменения планировались таким образом, чтобы минимизировать изменения на других уровнях протокольного стека TCP/IP. В результате размер IP-адреса увеличен до 128 бит. Даже с учетом неэффективности использования адресного пространства, являющейся оборотной стороной результативности маршрутизации и автоматического конфигурирования, этого достаточно, чтобы обеспечить объединение миллиарда сетей, как того требовали документы IETF (**Специальная комиссия интернет-разработок** (Internet Engineering Task Force, **IETF**)) - открытое международное сообщество проектировщиков, ученых, сетевых операторов и провайдеров, созданное IAB в 1986 г., которое занимается развитием протоколов и архитектуры Internet.

Обеспечена возможность простого и гибкого автоматического конфигурирования адресов для сетей произвольного масштаба и сложности. IPv6 является расширяемым протоколом, причем поля расширений (дополнительные заголовки) могут добавляться без снижения эффективности маршрутизации.

2.13. Протоколы транспортного уровня Internet

В Internet транспортный уровень представлен двумя протоколами: **TCP** (**Transport Control Protocol** - протокол контроля передачи) и **UDP** - протокол передачи датаграмм. Если предыдущий уровень (сетевой) определяет только правила доставки информации, то транспортный уровень отвечает за целостность доставляемых данных.

Протоколы транспортного уровня могут решать проблему негарантированной доставки сообщений ("дошло ли сообщение до адресата?"), а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные.

Протокол TCP. Это "гарантированный" транспортный механизм с предварительным установлением соединения, предоставляющий приложению безошибочный поток данных, перезапрашивающий дан-

ные в случае потери и устраняющий дублирование данных. TCP позволяет регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. TCP гарантирует, что полученные данные сформированы в той же последовательности, в которой они были отправлены. В этом его главное отличие от UDP.

Протокол UDP. Это протокол передачи датаграмм без установления соединения. Также его называют протоколом "ненадежной" передачи, в смысле невозможности удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. В приложениях, требующих гарантированной передачи данных, используется протокол TCP.

UDP обычно применяется в таких приложениях, как потоковое видео, где допускается потеря пакетов, а повторный запрос затруднен или не оправдан, либо в приложениях вида запрос-ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.

3. ГЛОБАЛЬНЫЕ СЕТИ И ИНТЕРНЕТ

3.1. Общая характеристика сети Internet

Сеть Internet - это сеть сетей, объединяющая как локальные, так и глобальные сети. С технической точки зрения Internet - объединение транснациональных компьютерных сетей, работающих по самым разнообразным протоколам, связывающим всевозможные типы компьютеров, физически передающих данные по телефонным проводам и оптоволокну, через спутники и радиомодемы. Таким образом, Internet состоит из множества компьютеров, соединенных между собой линиями связи, и установленных на этих компьютерах программ. Пользователи Internet подключаются к сети через оборудование специальных организаций - поставщиков услуг (*провайдеров*). К глобальной сети могут быть подключены как отдельный компьютер, так и локальная сеть. В последнем случае все пользователи локальной сети могут обращаться к услугам Internet, хотя линией связи с Internet соединен лишь один узел. Соединение может быть постоянным или временным (коммутируемым). Провайдеры имеют множество линий для подключения пользователей и высокоскоростные линии для связи с остальной частью Internet. Нередко мелкие поставщики подключены к более крупным, а компьютеры, подключенные к Internet, называют узлами, или хостами.

Наряду с Internet, используются внутренние сети предприятий, доступные только ее сотрудникам, работающие по протоколам стека TCP/IP и называемые *Интранет (Intranet)*. Такая система дает возможность создавать внутрикорпоративные информационные системы с рядом функциональных задач, позволяющих наиболее полно осуществлять корпоративные коммуникации между сотрудниками, отделами, представительствами компании.

Официальная документация по Internet излагается в документах RFC (Request for Comments). Документы с таким названием содержат в себе материалы по Internet-технологиям, которые доведены до уровня стандарта или близки к этому уровню. Информацию по данному вопросу можно найти по адресу: http://www.rfc-editor.org/ или http://www.ietf.org/rfc.html. Все разработчики должны придерживаться этой документации, но на практике не всегда так происходит.

3.1.1. Универсальные указатели ресурсов

При работе в Internet чаще всего используются не просто доменные адреса, а универсальные указатели (идентификаторы, локаторы) ресурсов, называемые URL - Universal Resource Locator. URL - это адрес и имя ресурса в Internet вместе с указанием того, с помощью какого протокола следует к нему обращаться. Понятие URL стало использоваться с появлением технологии WWW.

За основу при написании URL приняты правила системы Unix, которая претерпела естественные расширения за счет приписывания к существующей схеме адресации файлов имени протокола доступа к заданному ресурсу, затем - имени компьютера, где расположен ресурс, а справа - после служебных меток (#,?) - имени метки внутри файла или элементов поискового запроса.

Для разъяснения этих понятий проведем аналогию между системами Dos и Unix. Схема адресации в иерархически организованных файловых системах, таких как Dos (Windows) и Unix, позволяет однозначно идентифицировать заданный файл путем указания его имени и пути к нему.

Пример.

В DOS: *c:\dos\progr\file1.txt* **-** файл с именем *file.txt* находится на диске *c:* в каталоге *dos,* в подкаталоге *progr***.**

В Unix: */users/data/Letters.html* - файл с именем *Letters.html* расположен в корне, в директории *users*, подкаталоге *data***.**

Схемы адресаций похожи, за исключением: в Unix слэш прямой, эта система чувствительна к регистру в именах, в расширении файлов в Unix может быть более трех символов. Пример адресации:

http: //www.citmgu.ru/users/data/Letters.html#Mark1.

В примере содержится обращение по протоколу HTTP к WWW - серверу с доменным именем zitmgu.ru с попыткой доступа к файлу Letters.html с поисковой меткой Mark1.

Именно в таком виде и вводятся строки запроса на ресурс в специально отведенном поле браузера, после чего нажатие клавиши ENTER инициирует соединение и загрузку. В основу построения адреса ресурса в сети заложены следующие понятные принципы:

- расширяемость - новые адресные схемы должны вписываться в существующий синтаксис URL;
- полнота - по возможности любая из существующих схем должна быть описана посредством URL;
- читаемость - адрес должен быть легко читаем человеком, что вообще характерно для технологии WWW.

Таким образом, в URL первым ставится идентификатор протокола или схемы ресурса (например, HTTP), за ним ставится двоеточие, после чего указывается путь к ресурсу, т.е. доменный адрес машины, на которой установлен сервер HTTP и остаток пути к файлу на этом сервере.

3.1.2. Прикладной уровень Internet

На данном уровне работает большинство сетевых приложений. Эти программы имеют свои собственные протоколы обмена информацией, например, HTTP для WWW, FTP (передача файлов), SMTP (передача почты), DNS (преобразование символьных имен в IP-адреса) и многие другие. В массе своей эти протоколы работают поверх TCP или UDP (используют их на транспортном уровне) и привязаны к определенному порту. По номеру порта транспортные протоколы определяют, какому приложению передать содержимое пакетов. Порты могут принимать значение от 0 до 65538.

Номера портам присваиваются таким образом: имеются стандартные номера (например, номера 20, 21 закреплены за сервисом FTP, 23 - за TELNET, 80 - за HTTP), а менее известные приложения пользуются произвольно выбранными локальными номерами (как правило, больше 1024), некоторые из них также зарезервированы.

К прикладному уровню относятся протоколы **DHCP, FTP, TELNET, FINGER, GOPHER, HTTP, HTTPS, IMAP, IMAPS, SNMP, IRC, NFS, NNTP, NTP, POP3, POPS, QOTD, RTSP, XDMCP, SMTP.** Рассмотрим основные протоколы прикладного уровня.

Протокол HTTP (Hyper Text Transfer Protocol). Это протокол обмена гипертекстовой информацией. Сервер WWW (Apache, **IIS**) обрабатывает запросы клиента на получение файла (в самом простом случае). Взаимодействие клиента и сервера по протоколу HTTP приведено на рис. 19.

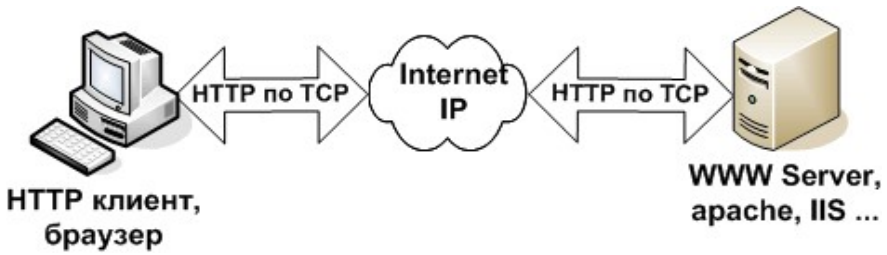

Рис. 19. **Взаимодействие клиента и сервера по протоколу HTTP**

На рисунке видно, что HTTP использует при передаче данных по сети протокол TCP (работает поверх TCP). Протокол HTTP определяет запрос-ответный способ взаимодействия между программой-клиентом и программой-сервером в рамках технологии World Wide Web.

Протокол FTP. Служба FTP (от протокола **File Transfer Protocol**). Предназначена для обмена файлами и построена по схеме "клиент-сервер".

Клиент посылает запросы серверу и принимает файлы. Сервер FTP (Apache, IIS) обрабатывает запросы клиента на получение файла. Схема взаимодействия клиента и сервера по протоколу FTP приведена на рис. 20.

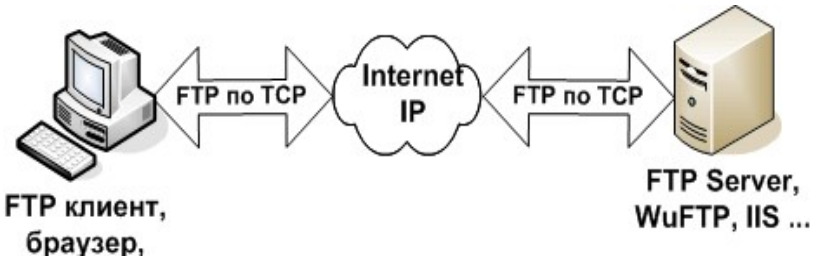

Рис. 20. **Взаимодействие клиента и сервера по протоколу FTP**

FTP отличается от других протоколов тем, что он использует два TCP соединения для передачи файла.

Управляющее соединение - соединение для посылки команд серверу и получение ответов от него. Соединение данных - соединение для передачи файлов. Схема двух каналов соединения по протоколу FTP приведена на рис. 21.

Протокол SNMP. Один из основных протоколов прикладного уровня (***Simple Network Management Protocol*** - простой протокол управления сетью). Это протокол управления сетями на основе архитектуры TCP/IP.

В настоящее время SNMP является базовым протоколом управления сети Internet. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети (главные машины, шлюзы и маршрутизаторы, терминальные серверы), которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами. SNMP различных версий посвящен целый ряд рекомендаций проблемной группы проектирования Internet (RFC).

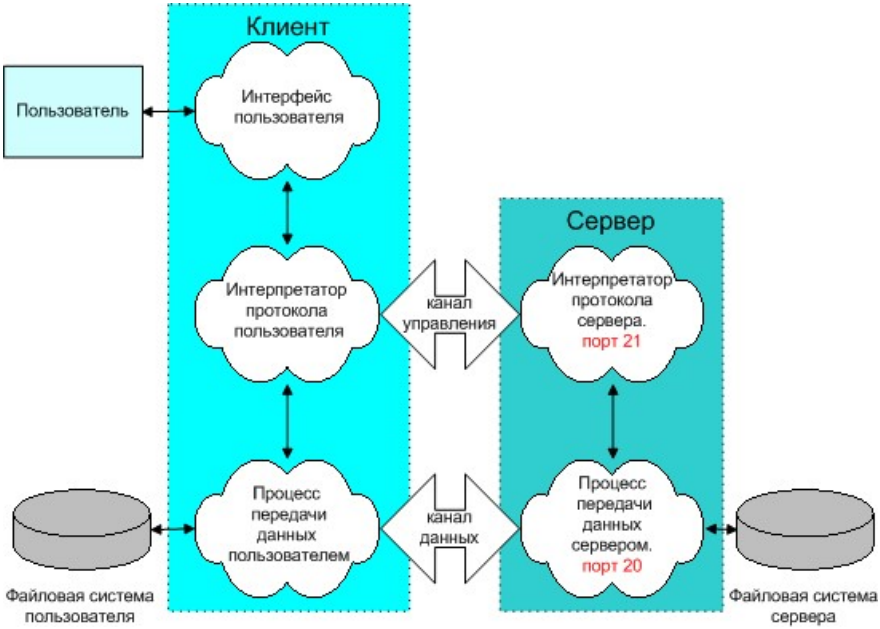

Рис. 21. **Схема двух каналов соединения по протоколу FTP**

Протоколы электронной почты. Основными почтовыми протоколами являются:

SMTP (Simple Mail Transfer Protocol). Простой протокол передачи почты используется для отправки почты как клиентом на сервер, так и сервером на другой сервер. Основной недостаток протокола - отсутствие аутентификации и "докачки" (как в FTP, HTTP) сообщений, т.е. если вы посылаете большое письмо (более 10 Мбайт), то в случае разрыва соединения ваше сообщение придется передавать заново, и, возможно, так до бесконечности. Поэтому большие письма необходимо резать на части. Порт по умолчанию - 25.

POP3 (Post Office Protocol). Используется для приема почты клиентом с сервера. Порт по умолчанию - 110.

IMAP4 (Internet Message Access Protocol). Позволяет клиентам получать доступ и манипулировать сообщениями электронной почты на сервере. Был разработан для замены POP3. Порт по умолчанию - 143.

Электронная почта во многом похожа на обычную почтовую службу. Схема функционирования электронной почты приведена на рис. 22. Сервер электронной почты обрабатывает сообщения (сортирует) и отправляет локальному адресату или удаленному серверу (почтовому отделению).

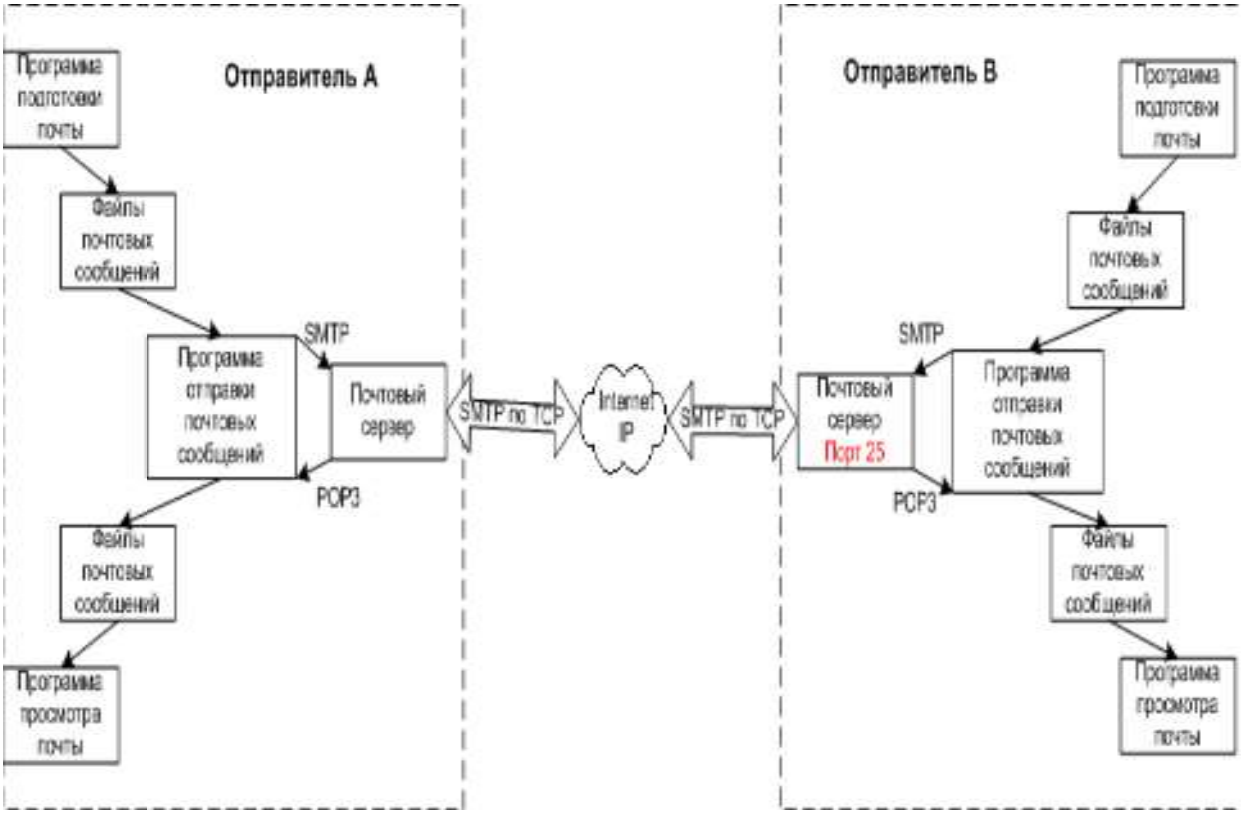

Рис. 22. **Схема отправки и получения почты**

В данном пособии рассматриваются подробности функционирования только основных протоколов прикладного уровня в Internet. Материалы о протоколах можно найти в [http://ru.wikipedia.org/wiki].

3.2. Сервисы Internet

Нельзя ввести сколько-нибудь жесткую или определенную классификацию сервисов Internet. Основная причина - уникальность каждого сервиса и одновременная неотделимость его от остальных. Каждый сервис характеризуется свойствами, часть которых объединяет его с одной группой сервисов, а другая часть с другой группой. Наиболее подходящим для классификации сервисов Internet является деление на сервисы интерактивные, прямого и отложенного чтения. Эти группы объединяют сервисы по большому числу признаков. Сервисы, относящиеся к классу *отложенного чтения,* наименее требовательны к ресурсам компьютеров и линиям связи. Основным признаком этой группы выступает та особенность, что запрос и получение информации могут быть достаточно сильно разделены по времени. Сюда относится, например, электронная почта. Сервисы *прямого обращения* характеризует то, что информация по запросу возвращается немедленно, однако от получателя информации не требуется немедленной реакции. Сервисы, где требуется немедленная реакция на полученную информацию, т.е. когда получаемая информация является, по сути дела, запросом, относятся к *интерактивным сервисам*. Для пояснения вышесказанного можно заметить, что в обычной связи аналогами сервисов интерактивных, прямых и отложенного чтения являются, например, телефон, факс и письменная корреспонденция. Рассмотрим самые популярные сервисы глобальной сети Internet.

3.2.1. Электронная почта

Электронная почта (e-mail) - первый из сервисов Internet, наиболее распространенный и эффективный. Электронная почта - типичный сервис отложенного чтения **(*off-line*).** Вы посылаете сообщение, как правило, в виде обычного текста, адресат получает его на

свой компьютер через какой-то (возможно, достаточно длительный) промежуток времени и читает ваше сообщение тогда, когда ему будет удобно. E-mail очень похож на обычную бумажную почту, обладая теми же достоинствами и недостатками.

Итак, электронная почта повторяет достоинства (простота, дешевизна, возможность пересылки нетекстовой информации, возможность подписать и зашифровать письмо) и недостатки (негарантированное время пересылки, возможность доступа третьих лиц во время пересылки, неинтерактивность) обычной почты. Однако у них есть и существенные отличия. Стоимость пересылки обычной почты очень сильно зависит от того, куда, в сколь удаленную точку планеты она должна быть доставлена, ее размера и типа. Для электронной почты такой зависимости или нет, или она довольно невелика. Электронное письмо можно шифровать и подписывать гораздо более надежно и удобно, нежели бумажное - для последнего, строго говоря, вообще нет общепринятых средств шифрования. Скорость доставки электронных писем гораздо выше, чем бумажных, и минимальное время их прохождения несравнимо меньше. E-mail универсален - множество сетей во всем мире, построенных на совершенно разных принципах и протоколах, могут обмениваться электронными письмами с Internet, получая тем самым доступ к прочим его ресурсам. Практически все сервисы Internet, использующиеся обычно как сервисы прямого доступа (*on-line*), имеют интерфейс к электронной почте, так что даже если у вас нет доступа к Internet в режиме on-line, вы можете получать большую часть информации, хранящейся в Internet, посредством дешевой электронной почты. Скорость доставки сообщений электронной почты сильно зависит от того, каким образом она передается. Путь электронного письма между двумя машинами, непосредственно подключенными к Internet, занимает секунды, и при этом вероятность потери или подмены письма минимальна.

3.2.2. Система гипермедиа WWW

WWW (*World Wide Web - всемирная паутина*) - самый популярный и интересный сервис Internet сегодня, самое популярное и удобное средство работы с информацией. Больше половины потока данных Internet приходится на долю WWW.

Сегодня WWW - самая передовая технология Internet, и она уже становится массовой технологией - возможно, недалек тот день, ко-

гда каждый человек, знающий, что такое телефон, будет знать, что такое WWW.

WWW - информационная система, которой весьма непросто дать корректное определение. Вот некоторые из эпитетов, которыми она может быть обозначена: гипертекстовая, гипермедийная, распределенная, интегрирующая, глобальная. Ниже будет показано, что понимается под каждым из этих свойств в контексте WWW. WWW работает по принципу клиент-серверов: существует множество серверов, которые по запросу клиента возвращают ему гипермедийный документ - документ, состоящий из частей с разнообразным представлением информации (текст, звук, графика, трехмерные объекты и т.д.), в котором каждый элемент может являться ссылкой на другой документ или его часть. Ссылки эти в документах WWW организованы таким образом, что каждый информационный ресурс в глобальной сети Internet однозначно адресуется, и документ, который вы читаете в данный момент, способен ссылаться как на другие документы на этом же сервере, так и на документы (и вообще на ресурсы Internet) на других компьютерах. Причем пользователь не замечает этого и работает со всем информационным пространством Internet как с единым целым.

Ссылки WWW указывают не только на документы, специфичные для самой WWW, но и на прочие сервисы и информационные ресурсы Internet. Более того, большинство программ-клиентов WWW (browsers, навигаторы) не просто понимают такие ссылки, но и являются программами-клиентами соответствующих сервисов: ftp, gopher, сетевых новостей Usenet, электронной почты и т.д.

Таким образом, программные средства WWW являются универсальными для различных сервисов Internet, а сама информационная система WWW играет интегрирующую роль.

Некоторые термины, использующиеся в WWW:

- *html (hypertext markup language, язык разметки гипертекста)* - формат гипермедийных документов, использующихся в WWW для представления информации. Формат этот не описывает то, как документ должен выглядеть, но определяет его структуру и связи. Внешний вид документа на экране пользователя определяется программой - *навигатором (браузером),* и если вы работаете за графическим или текстовым терминалом, то в каждом случае документ будет выглядеть по-своему, но структура его останется неизменной, поскольку она задана форматом html. Имена файлов в формате html имеют расширение *.html (.htm);*

• *http (hypertext transfer protocol, протокол передачи гипертекста*) - название протокола, по которому взаимодействуют клиент и сервер WWW;

• WWW - сервис *прямого доступа,* требующий полноценного подключения к Internet и, более того, часто требующий быстрых линий связи, если документы, которые вы читаете, содержат много графики или другой нетекстовой информации.

Децентрализованность WWW вносит некоторые затруднения - например, сегодня стандартом становятся не те расширения языка html, которые лучше, но те, которые привносятся самыми популярными навигаторами, такими как Vicrosoft Internet Explorer, Netscape Navigator. Децентрализованность несет и множество других проблем: отсутствие общего каталога серверов и средств тотального поиска по ним. Однако эта проблема успешно решается - сегодня есть и каталоги, и поисковые системы, которые, если и не являются глобальными, но тем не менее охватывают достаточно большую часть документов WWW, чтобы быть полезными и успешно применяться для поиска информации.

3.2.3. FTP - передача файлов

Еще один широко распространенный сервис Internet - FTP (File Transfer Protocol). Расшифровывается эта аббревиатура как протокол передачи файлов, но при рассмотрении ftp как сервиса Internet имеется в виду не просто протокол, но именно сервис - доступ к файлам в файловых архивах. Вообще говоря, ftp - стандартная программа, работающая по протоколу tcp, всегда поставляющаяся с операционной системой. Ее исходное предназначение - передача файлов между разными компьютерами, работающими в сетях *tcp/ip*: на одном из компьютеров работает программа-сервер, на втором пользователь запускает программу-клиент, которая соединяется с сервером и передает или получает по протоколу *ftp* файлы. Предполагается, что пользователь зарегистрирован на обоих компьютерах и соединяется с сервером под своим именем и со своим паролем на этом компьютере. Протокол *ftp* оптимизирован для передачи файлов. Данная черта и послужила причиной того, что программы ftp стали частью отдельного сервиса Internet. Дело в том, что сервер ftp зачастую настраивается таким образом, что соединиться с ним можно не только под своим

именем, но и под условным именем anonymous - аноним. Тогда вам становится доступна не вся файловая система компьютера, но некоторый набор файлов на сервере, которые составляют содержимое сервера anonymous ftp - *публичного файлового архива*.

Если кто-то хочет предоставить в публичное пользование файлы с информацией, программами и прочим, то ему достаточно организовать на своем компьютере, включенном в Internet, сервер anonymous ftp. Сделать это несложно, программы-клиенты ftp есть практически на любом компьютере - поэтому сегодня публичные файловые архивы организованы в основном как серверы anonymous ftp. На таких серверах в настоящее время доступно огромное количество информации и программного обеспечения. Практически все, что может быть предоставлено пользователям в виде файлов, доступно с серверов anonymous ftp. Это и свободно распространяемые программы, и демонстрационные версии, мультимедиа или просто тексты - законы, книги, статьи, отчеты, рефераты.

Таким образом, если вы, например, хотите представить миру демонстрационную версию вашего программного продукта, anonymous ftp является удачным решением такой задачи. Если, с другой стороны, вы хотите найти, скажем, последнюю версию вашей любимой свободно распространяющейся программы, то искать ее нужно именно на серверах ftp.

Несмотря на распространенность, у ftp есть и множество недостатков. Программы-клиенты ftp могут быть не всегда удобны и просты в использовании. Не всегда можно понять, а что это за файл перед вами - то ли это тот файл, что вы ищете, то ли нет. Нет простого и универсального средства поиска на серверах anonymous ftp - хотя для этого и существует специальный сервис archie, но это независимая программа, неуниверсальная и не всегда применимая. Программы ftp довольно стары, и некоторые их особенности, бывшие полезными при рождении, не очень понятны и нужны сегодня. Так, например, для передачи файлов есть два режима - бинарный и текстовый, и если вы вдруг неправильно выбрали режим, то передаваемый файл может быть поврежден. Описания файлов на сервере выдаются в формате операционной системы сервера, а список файлов операционной системы UNIX может привести в недоумение пользователя Windows. Проблема тут в том, что со списком файлов выдается лишняя информация, а слишком много знать всегда вредно. Серверы ftp нецентрализованы, и это несет свои проблемы.

Несмотря на все это, серверы anonymous ftp сегодня - стандартный путь организации публичных файловых архивов в Internet. Вы можете также обеспечивать доступ к файлам под паролем - напри-

мер, своим клиентам. Ftp-сервис - это сервис прямого доступа, требующий полноценного подключения к Internet, но возможен и доступ через электронную почту, существуют серверы, которые могут прислать вам по электронной почте файлы с любых серверов anonymous ftp. Однако это может быть весьма неудобно, ибо такие серверы сильно загружены, и ваш запрос может долго ждать своей очереди. Кроме того, большие файлы при отсылке делятся сервером на части ограниченного размера, посылаемые отдельными письмами, и если одна часть из сотни потеряется или повредится при передаче, то остальные 99 тоже окажутся ненужными.

В Internet есть много других сервисов: телеконференции, Telnet, Gopher, Wais и другие, на сегодняшний день менее популярные и реже используемые. Информацию о них можно найти в рекомендуемой литературе.

3.3. Виды подключения к Internet

Для подключения к Internet выбирается Internet-провайдер, предоставляющий услуги Internet. С ним заключается договор на предоставление услуг, оговариваются виды услуг и их стоимость. При выборе провайдера следует учитывать качество его услуг, стоимость (примерно одинакова для всех провайдеров), качество оборудования, опыт ваших знакомых при работе с тем или другим провайдером и др. Можно, не заключая договора, поработать с несколькими провайдерами, покупая на короткий срок абонентские карточки, а далее уже заключать договор с лучшим, на ваш взгляд, провайдером.

Используются следующие виды подключения: Dial-up доступ, технология ADSL, технология xDSL, Выделенный Internet, Спутниковый Internet, Мобильный Internet, GPRS Internet, Локальная сеть.

Dial-up. Это способ подключения к Internet посредством модема и коммутируемой линии городской телефонной сети. Скорость передачи данных до 56 Кбит/с, зависит от качества телефонных линий. Данный способ соединения имеет ряд преимуществ: возможность использования уже существующей линии для доступа в Internet; низкая стоимость абонентского оборудования; низкая стоимость и простота подключения. Самым большим недостатком этого способа является низкая скорость передачи.

Технология ADSL. Аббревиатура ADSL (Asymmetric Digital Subscriber Line) расшифровывается как "Асимметричная цифровая абонентская линия", что подчеркивает изначально заложенное в этой технологии различие скоростей обмена в направлениях к абоненту и обратно. Асимметричность ADSL подразумевает передачу больших объемов информации к абоненту (видео, массивы данных, программы) и небольших объемов от абонента (в основном команды и запросы). Оборудование ADSL, размещенное на АТС, и абонентский ADSL-модем, подключаемые к обоим концам телефонной линии, образуют три канала:

- высокоскоростной канал передачи данных из Сети в компьютер (скорость от 32 Кбит/с до 8 Мбит/с);
- скоростной канал передачи данных из компьютера в сеть (скорость - от 32 Кбит/с до 1 Мбит/с);
- простой канал телефонной связи, по которому передаются обычные телефонные разговоры. Величина скорости передачи данных при этом зависит от длины и качества телефонной линии.

Асимметричный характер скорости передачи данных вводится специально, так как удаленный пользователь Internet обычно загружает данные из сети в свой компьютер, а в обратном направлении идут либо команды, либо поток данных существенно меньшей скорости. Для получения асимметрии скорости полоса пропускания абонентского окончания делится между каналами также асимметрично. На дальнем конце абонентского окончания должен располагаться так называемый мультиплексор доступа DSLAM. Этот мультиплексор выделяет подканалы из общего канала и отправляет голосовой подканал на АТС, а высокоскоростные каналы данных направляет на маршрутизатор, подключенный к DSLAM. Одно из главных преимуществ технологии ADSL состоит в том, что поддержка голоса никак не отражается на параллельной передаче данных по двум быстрым каналам. Причина подобного эффекта - основанность ADSL на принципах разделения частот, благодаря чему голосовой канал надежно отделяется от двух других каналов передачи данных.

Технология DSL. XDSL - в буквальном переводе на русский язык - это цифровая абонентская линия (Digital Subscriber Line). Возник этот термин с появлением ISDN (Integrated Service Digital Network) - цифрового абонентского доступа, реализованного с приходом в 1980-х гг. новых цифровых автоматических телефонных станций (цифровых АТС). Чаще всего термин DSL использовался в

контексте ISDN BRI (Basic Rate Interface) - цифрового доступа со скоростью 160 Кбит/с. В данное время термин почти полностью утратил связь с линией ISDN BRI и означает технологию для высокоскоростной передачи дискретных сигналов по физической линии (обычно медному проводу). Шире DSL - это совокупность технических средств, включающих абонентскую линию связи ("витую пару") и цифровую систему передачи, или так называемые модемы, обеспечивающие дуплексную (двунаправленную) передачу по абонентской линии цифровых сигналов. Сегодня имеется множество разных "DSL-подобных" методов передачи информации по медному проводу. Всех их условно объединяют в семейство xDSL-технологий. В линиях, организованных на базе xDSL-оборудования, трафик передается только в цифровом виде, а xDSL чаще используется для организации доступа конечных пользователей к сетям передачи данных общего пользования, например, Internet. В последнее время инженерами были отработаны разные варианты внедрения систем высокоскоростного доступа для массового пользователя. Технология xDSL работает на существующих телефонных линиях и обеспечивает скорость доступа до 115,2 Кбит/с. Телефон и Internet работают синхронно по одной линии. Обеспечить такую скорость удается благодаря использованию самых современных телекоммуникационных технологий и решений при организации цифровой связи. Модемы устанавливаются перед АТС таким образом, что связь с абонентским модемом совершается не через коммутационное оборудование АТС (как при Dial-up), а фактически через непосредственное соединение. Ваша телефонная линия поступает на АТС уже после оборудования xDSL, которое в обход АТС включено цифровым каналом в сеть Internet. Важной особенностью оборудования xDSL является то, что при установке его на вашу линию полностью сохраняется возможность пользования всеми услугами традиционной телефонной сети (в том числе определителем номера, факсом или обычным аналоговым модемом) даже во время передачи данных. Дело в том, что ваш голос и голос вашего собеседника оцифровываются и передаются xDSL-модемами синхронно с другими данными. Вы сможете разговаривать по обычному телефону и работать в Internet синхронно, т.е. соединение с Internet во время разговора сохранится, а скорость его лишь немного снизится. Высокая надежность телефонной связи обеспечивается тем, что при отключении электропитания, в том числе аварийном, xDSL-модемы отключатся и ваш телефон будет работать в обычном режиме. Кроме того, при использовании xDSL-модемов благодаря цифро-

вой передаче телефонных разговоров повышается конфиденциальность связи. Подключение со скоростью 115,2 Кбит/с к серверам Internet удовлетворяет многих пользователей по соотношениям продуктивности и стоимости для малых или средних офисов и домашних пользователей.

Выделенный Internet. Это высококачественный, скоростной и постоянный доступ в Internet по отдельному кабелю. Чтобы соединиться с Internet по выделенной линии, достаточно просто включить компьютер. Internet доступен до тех пор, пока компьютер включен. Выделенный Internet мало используется для подключений домашних пользователей, поскольку стоимость прокладки выделенной линии высока, а при наличии ADSL и xDSL достаточно эффективно используются и имеющиеся телефонные линии.

Спутниковый Internet. Спутниковый Internet - это самый экономичный способ высокоскоростного подключения к глобальной Сети. По сравнению с традиционными выделенными линиями стоимость получения одного Мегабайта данных в 2-9 раз ниже и составляет в среднем всего 80-90 копеек. При этом спутниковое соединение обеспечивает столь же быструю передачу данных, как и выделенная линия - до нескольких Мбит/с (это примерно в 100 раз быстрее обычного модема). Спутниковая связь достаточно надежна. Несмотря на большое количество пользователей, спутниковый канал "перегрузить" очень сложно. Ведь те же самые спутники используются для передачи десятков цифровых телеканалов, а для этого нужна несравнимо большая пропускная способность. В случае необходимости провайдер спутникового Internet расширяет свою полосу. Обычно в его распоряжении находится полоса в несколько десятков Мбит/с, и каждому пользователю из нее выделяется до нескольких Мбит/с.

Услугами спутникового Internet можно пользоваться в любой географической точке, расположенной в обширной зоне обслуживания спутника. Передача данных через спутник носит односторонний характер: вы можете только получать данные. Для передачи ваших запросов на какую-либо информацию в сети, а также исходящих от вас данных (например, ваших электронных писем) нужно использовать любой вид наземного соединения. Это может быть кабельное соединение (Ethernet, ADSL), радиолиния, или, как это часто бывает, обычный Dial-Up модем и даже мобильный телефон (GPRS). Вся входящая к вам информация будет поступать через высокоскоростной спутниковый канал. Поскольку объем исходящей от вас информации намного меньше, чем объем входящей к вам на компьютер

(примерно в 10 раз), исходящая от вас информация обычно не тарифицируется местными провайдерами. Спутниковый Internet позволяет существенно снизить Ваши расходы на трафик при высокой скорости получения информации из сети.

Радиоканал. Радиоканал - беспроводное подключение с использованием радиоволн. Радиоканал позволяет подключить к сети домашний компьютер или локальную компьютерную сеть офиса (предприятия). По радиоканалу доступны все услуги сети, предоставляемые по кабельным каналам.

Организация беспроводной сети рассматривается в данном пособии в разделе "Беспроводные сети".

Локальная сеть. Подключение к Internet через локальную сеть является одним из самых используемых видов подключения к Internet любого учреждения, предприятия. Сейчас уже распространены домашние ЛВС, подключенные к глобальной сети. Одним из главных преимуществ для объединения в сеть является совместный выход в Internet, что делает подключение скоростным и более дешевым. В пособии подробно рассматриваетя ЛВС Ethernet и ее интеграция с Internet.

GPRS. Аббревиатура GPRS расшифровывается как **General Packet Radio Service.** Это своеобразная надстройка над обычной GSM сотовой сетью, которая позволяет передавать данные на существенно более высоких, чем в обычной GSM-сети, скоростях. Если в обычной GSM-сети можно получить максимум 14,4 Кбит/с, то теоретический максимум в GPRS составляет 171,2 Кбит/с при полном использовании. GPRS - это пакетная система передачи данных, функционирующая аналогично сети Internet. Весь поток данных отправителя разбивается на отдельные пакеты и затем доставляется получателю, где пакеты собираются воедино. Internet и GPRS объединяет не только пакетная передача данных. При начале GPRS-сессии каждому GPRS-терминалу, как и в Internet, присваивается свой уникальный адрес, протокол GPRS прозрачен для TCP/IP, поэтому интеграция GPRS-сети с Internet происходит незаметно для конечного пользователя.

Для передачи данных, помимо высокоэффективных алгоритмов кодирования, используется такая технология: терминалу автоматически выделяются не используемые в данный момент времени таймслоты, что позволяет оптимизировать загрузку сети. Такая схема влечет за собой "плавающие" скорости передачи данных у конкретной

базовой станции в зависимости от количества активных абонентов. Новая технология EDGE (Enhanced Data Rates for GSM Evolution) - это промежуточный этап между технологией GPRS и стандартами связи третьего поколения, например, технологией UMTS. EDGE позволяет получать доступ к сети с еще большей скоростью, по сравнению с GPRS скорость соединения через EDGE возрастает примерно в 3 раза. Такие результаты были, в частности, достигнуты во время тестирования этой технологии. Если GSM поддерживает скорость 9,6 Кбит/с, то в GPRS она увеличивается до 172 Кбит/с, а в EDGE до 384 Кбит/с (это теоретическое значение). А в реальности средняя скорость передачи данных составляет 100 - 120 Кбит/с с пиковыми значениями до 200-220 Кбит/с.

Основным преимуществом EDGE перед GPRS является именно скорость. Таким образом, при той же тарификации абонент получает возможность передачи больших объемов данных за то же время и при том же количестве используемых таймслотов в радиоэфире, что и через GPRS. Тарификация опять же зависит не от длительности соединения, а от объема переданных данных. В итоге использование услуг доступа в Internet, к WAP-ресурсам (WEB - интерфейс мобильной связи), передача MMS-сообщений становятся более эффективными. MMS - Multimedia Message Service - служба мультимедийных сообщений - это система, позволяющая посылать и принимать изображения, мелодии, видео при помощи сотового телефона.

3.4. Вопросы информационной безопасности в сети

Сеть или компьютер, подключенные к Internet, подвергаются гораздо большему количеству опасностей. Чтобы представить, от чего защищаться, зачем и чем, попытаемся классифицировать эти угрозы. Рассмотрим кратко каждую из них.

Хакеры. Предположим, вы - обычный пользователь Internet. Дома имеете беспроводную сеть из настольного компьютера и ноутбука. Вы интересны любому хакеру своими регистрационными данными. Перехватив их, злоумышленник может пользоваться сетью Internet за ваш счет. Если вы пользуетесь какой-либо онлайновой платежной системой, хакер постарается узнать ваш пароль и скопировать с ва-

шего компьютера файл с ключами для доступа к этой системе. Для хакеров также может быть интересна ваша электронная почта: некто хочет почитать ее или отправить письмо от вашего имени. Некоторые пользователи Internet хранят на жестком диске незашифрованные данные к кредитной карточке, что тоже может представлять интерес для хакера. Так что, даже если вы простой пользователь, для хакеров вы тоже можете представлять интерес.

Сетевые черви и вирусы. Это вредоносные программы. Бывают вирусы, распространяющиеся по сети, и те, что размножаются, инфицируя другие программы. Вирус (почтовый червь) можно получить по электронной почте в виде вложенного файла. Internet-червь может проникнуть в компьютер прямо из сети. Почтовые черви очень изобретательны. Можно получить сообщение, вполне безопасное с виду, например, маркированное как ответ на ваше сообщение или как сообщение с почтового сервера. В письме может быть текст, предлагающий вам открыть интересное вложение, которое выглядит как файл .jpg. На самом деле это может быть не картинка, а вредоносная программа. Черви, как и хакеры, применяют методы социальной инженерии, прикидываясь полезными, интересными, нужными. Поэтому, если у вас есть хоть малейшее сомнение, не открывайте вложения неожидаемых почтовых сообщений.

Вирус может быть разрушительным оружием для вашего компьютера: испортить или стереть данные, замедлить работу, удалить нужные файлы, украсть информацию (переслать по определенному адресу) и т.д. Сетевые черви в последнее время занимаются не похищением информации (хотя такое случается), а превращением компьютеров в "зомби". Такие компьютеры могут использоваться злоумышленниками, например, для рассылки спама и для организации масштабных атак на определенные ресурсы.

Краткий обзор антивирусных программ. В настоящее время перечень доступных антивирусных программ весьма обширен. Они различаются как по цене (от весьма дорогих до абсолютно бесплатных), так и по своим функциональным возможностям. Наиболее мощные (и, как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании поставить заслон практически любому виду зловредных программ. Вот типовой (но, возможно, неполный) перечень тех функций, которые могут выполнять такие антивирусные пакеты:

- сканирование памяти и содержимого дисков по расписанию;

• сканирование памяти компьютера, а также записываемых и читаемых файлов в реальном режиме времени с помощью резидентного модуля;

• выборочное сканирование файлов с измененными атрибутами;

• распознавание поведения, характерного для компьютерных вирусов;

• блокировка и/или удаление выявленных вирусов;

• восстановление зараженных информационных объектов;

• принудительная проверка подключенных к корпоративной сети компьютеров;

• удаленное обновление антивирусного программного обеспечения и баз данных с информацией о вирусах, в том числе автоматическое обновление баз данных по вирусам через Internet;

• фильтрация трафика Internet на предмет выявления вирусов в передаваемых программах и документах;

• выявление потенциально опасных Java-апплетов и модулей ActiveX;

• ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

К наиболее мощным и популярным сегодня (в России) антивирусным пакетам относятся:

Антивирус Dr.Web. Доктор Веб - одна из самых известных и популярных отечественных антивирусных программ. Имеет эвристический анализатор, позволяющий с большой долей вероятности обнаруживать неизвестные вирусы. Программа допускает автоматическую загрузку из Internet новых баз данных вирусов и автообновление самой программы, что позволяет оперативно реагировать на появление новых вирусов.

Антивирус N3OD2. Очень быстро работающая антивирусная программа, эффективно защищающая от всех видов вирусов и "шпионских" программ. NOD32 обладает всеми возможностями, характерными для современных средств защиты компьютера, причем по некоторым очень важным параметрам NOD32 превосходит абсолютное большинство популярных антивирусных программ. Это единственный антивирус в мире, который уже более 7 лет не пропустил ни один активный на момент тестирования вирус, а также не менее мощный и встроенный виртуальный эмулятор для обнаружения полиморфных вирусов.

Norton AntiVirus. Это одна из самых известных в мире антивирусных программ. Производится американской компанией Symantec.

Данный антивирус находит и удаляет вирусы и программы-шпионы, автоматически блокирует программы-шпионы, не позволяет рассылать зараженные письма, автоматически распознает и блокирует вирусы, программы-шпионы и троянские компоненты, обнаруживает угрозы, скрытые в операционной системе, выполняет функцию защиты от интернет-червей, функцию просмотра электронной почты.

Panda Antivirus. Panda Antivirus 2007 делает защиту ПК максимально простой: антивирус автоматически блокирует и уничтожает все типы вирусов и шпионов, так что можно пользоваться Internet и электронной почтой без риска для безопасности. Продукт представляет легкое и высокоэффективное решение с высокой скоростью работы.

Антивирус Касперского. Антивирус Касперского - одна из популярнейших и наиболее качественных антивирусных программ. За счет специального алгоритма работы у нее очень высокий процент определения вирусов, в том числе и еще неизвестных. Антивирус Касперского умеет проверять на вирусы почтовые базы данных и получаемые письма вместе с приложениями к ним, очень хорошо определяет макровирусы, внедренные в документы Microsoft Office, а также проверяет наиболее популярные форматы архивов.

Популярность перечисленных выше пакетов обусловлена прежде всего тем, что в них реализован комплексный подход к борьбе с вредоносными программами. Последние версии антивирусных программ содержат в своем составе также и средства борьбы с вредоносными программами, проникающими из сети.

4. ОБЛАЧНЫЕ И МОБИЛЬНЫЕ ТЕХНОЛОГИИ. ЭЛЕКТРОННЫЕ СЕРВИСЫ

4.1. Создание облачных технологий

Слово "облако" (cloud) использовалось в 1990-х гг. для метафорического обозначения Internet: тогда Глобальная сеть представлялась чем-то загадочным, неопределенным в своих пространственных границах, неотличимым от своих внутренних элементов и быстро изменяющимся. Зафиксированное в статье под заголовком "ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing" определение "облачных вычислений" гласит: "Это тот случай, когда информация постоянно хранится на серверах в Сети и временно сохраняется на стороне клиента - например, на настольных компьютерах, планшетах, ноутбуках, мини-компьютерах и так далее".

Впервые идею "облачных вычислений" озвучил Д. Ликлайдер в 1960 г. Его идея заключалась в том, что каждый человек на планете будет подключен к сети, из которой он будет получать не только данные, но и программы. Другой ученый, Джон Маккарти, высказал идею о том, что вычислительные мощности будут предоставляться пользователям как услуга.

В 1990-е гг. происходит быстрый рост глобальной сети - Internet, оказывающий косвенное влияние на развитие облачных технологий. Значительно увеличилась пропускная способность сетей, расширилась география охвата. Наряду с развитием компьютерных сетей усовершенствовались аппаратные технологии, появились многоядерные процессоры, значительно вырос объем хранилищ информации.

Появление первой технологии, близкой к современному пониманию термина "cloud computing", приписывается компании Salesforce.com, основанной в 1999 г. Данная компания стала первой компанией, предоставившей доступ к своему приложению через сайт, по сути, стала первой компанией, предоставившей свое программное обеспечение по принципу - программное обеспечение как сервис (SaaS). Следующим шагом стала разработка облачного веб-сервиса компанией Amazon в 2002 г. Данный сервис позволял хранить информацию и производить вычисления. В 2006 г. Amazon запустила

сервис под названием Elastic Compute cloud (EC2) как веб-сервис, который позволял его пользователям запускать свои собственные приложения. Следующим свою технологию постепенно ввела Google, начав с 2006 г. предложение SaaS-сервисов под названием Google Apps, а затем и модели предоставления платформы как сервиса (PaaS) под названием Google App Engine. И наконец, свое предложение анонсировала компания Microsoft, презентовав ее на конференции PDC в 2008 г. под названием Azure Services Platform.

Дуглас Минифи - ИТ-директор крупной компании The Schumacher Group, которая занималась управлением отделениями неотложной помощи больниц и организацией труда врачей. Перед ним встал вопрос: "Чем все-таки должна в первую очередь заниматься наша фирма - разрабатывать программное обеспечение или использовать его для управления медицинскими ресурсами?"

С этого вопроса и началось в The Schumacher Group исследование совершенно нового ИТ-феномена под названием "облачные вычисления". Тем не менее, большинство ИТ-директоров продолжают полагаться на собственные серверные инфраструктуры по одной простой причине: они не уверены, что облачные вычисления уже готовы для широкого выхода в свет. Причем, если верить сообщениям в посвященных этой технологии форумах, главный вопрос состоит вовсе не в том, достаточно ли она надежна для ИТ-сред. Гораздо больше ИТ-руководителей тревожат другие аспекты. Они не уверены в безопасности своих данных, которые оказываются в руках оператора "облака". Они считают, что не смогут эффективно управлять облачными ресурсами, подозревают, что провайдеры не раскрывают все детали поддерживающей облачную среду инфраструктуры, видят в новой технологии угрозу своим вычислительным центрам и даже персоналу. Все это в итоге сдерживает развитие рынка облачных вычислений.

Но что бы там ни говорили об облачных вычислениях, ясно одно: развитие этой технологии просто невозможно игнорировать. Стоит отметить, что идея аренды приложений, платформ разработки, вычислительных мощностей, хранилищ и любых других облачных сервисов повторяет путь Internet от экспериментальной системы к серьезному пользовательскому инструменту. Технология облачных вычислений способна в корне изменить облик информационных технологий.

Несмотря на колебания среди ИТ-директоров, все больше поставщиков облачных сервисов активно продвигают свои услуги в предвкушении грядущего прорыва в этой области. Самые зрелые

предложения поступают сегодня со стороны Amazon, Google и Salesforce.com, которые чуть ли не ежедневно добавляют в свои сервисы все новые функции.

IBM, которая подключилась к исследованиям Google в сфере облачных вычислений, проводит агрессивный маркетинг архитектуры Blue Cloud, специально разработанной для данной технологии. И некоторые крупномасштабные фирмы, стремясь не упустить шанс, заключают с Intel партнерские соглашения по созданию крупномасштабной тестовой системы облачных вычислений.

Некоторые компании уже сейчас предлагают операторам связи, кабельным компаниям и поставщикам услуг Internet богатый ассортимент аппаратных средств для реализации этой технологии.

Облачное хранилище данных - модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в Сети серверах, предоставляемых в пользование клиентам в основном третьей стороной. В противовес модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту в общем случае не видна. Данные хранятся, а равно и обрабатываются в так называемом облаке, которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически же такие серверы могут располагаться удаленно друг от друга географически, вплоть до расположения на разных континентах.

Другими словами, это своеобразный онлайн-сервис, предоставляющий возможность хранить файлы на удаленном сервере. То есть пользователь может загрузить документ в любое онлайн-хранилище и в будущем использовать его прямо из сервера. С точки зрения клиента, все операции происходят в одном месте, так называемом облаке. Однако на самом деле удаленный сервер чаще всего располагается в разных местах, а иногда и на разных континентах. Но это нисколько не затрудняет работу облачных сервисов, так как скорость работы зависит от клиента, а точнее, от скорости интернет-соединения у клиента, которая желательно не должна быть ниже 600 Кбит/с. Именно поэтому облачные сервисы появились совсем недавно, так как высокоскоростной Internet с предоставляемой скоростью не менее 1 Мбит/с появился в нашей стране.

Облачных хранилищ довольно много, и все они предоставляют различные возможности. Они бывают платные и бесплатные, рассчитаны на большой и на малый объем информации, поддержку разных

операционных систем и т.д. Единственное, в чем они сходны между собой, - в способе обработки информации.

Достоинства облачных вычислений: уменьшение затрат и увеличение эффективности ИТ-инфраструктуры. Обычные серверы средней компании загружены на 10-15 %. В одни периоды времени есть потребность в дополнительных вычислительных ресурсах, в другие эти дорогостоящие ресурсы простаивают. Используя необходимое количество вычислительных ресурсов в "облаке" в любой момент времени, компании сокращают затраты на оборудование и его обслуживание до 50 %, а также на приобретаемое программное обеспечение. Вместо приобретения пакетов программ для каждого локального пользователя компании покупают нужные программы в "облаке". Имеет место постоянное обновление программ, увеличение доступных вычислительных мощностей. Пользователи могут запускать более сложные задачи, с большим количеством необходимой памяти, места для хранения данных тогда, когда это необходимо. Облачные вычисления имеют доступ к программам и виртуальным компьютерам, который происходит при помощи веб-браузера или других средств доступа, устанавливаемых на любой персональный компьютер с любой операционной системой, а также обладают неограниченным объемом хранимых данных.

Недостатки облачных вычислений: плохо работают с медленным интернет-доступом. Многие облачные программы требуют хорошего интернет-соединения с большой пропускной способностью, могут работать медленнее, чем на локальном компьютере. Не все программы или их свойства доступны удаленно. Если сравнивать программы для локального использования и их облачные аналоги, последние пока проигрывают в функциональности. Безопасность данных может быть под угрозой (здесь ключевым является слово "может").

Все зависит от того, кто предоставляет облачные услуги. Если этот кто-то надежно шифрует данные, постоянно делает их резервные копии, уже не один год работает на рынке подобных услуг и имеет хорошую репутацию, то угрозы безопасности данных может никогда не случиться. Если данные в "облаке" потеряны, то они потеряны навсегда. Это факт. Но потерять данные в "облаке" гораздо сложнее, чем на локальном компьютере.

Несмотря на то, что количество плюсов превосходит минусы, в каждой конкретной ситуации они имеют большую важность или, наоборот, не имеют никакого значения.

4.2. Модели SaaS, PaaS, DaaS, IaaS

IaaS - услуга "Инфраструктура как сервис" - базовая облачная услуга, которую предоставляет любой провайдер. По сути это вычислительная инфраструктура - одна или несколько виртуальных машин без какого-либо дополнительного программного обеспечения. В этом случае провайдер несет ответственность за доступность виртуальной машины на уровне среды виртуализации.

PaaS - платформа как сервис - это по сути "инфраструктура + софт", которые необходимы для работы конечного приложения. Софт - это операционные системы, СУБД, всякого рода балансировщики и все, что потребует разработчик для запуска своего приложения. Здесь провайдер не просто отвечает за доступность виртуальной машины, а гарантирует работоспособность всего ПО, которое было перечислено.

SaaS - софт как сервис - это платформа + прикладное программное обеспечение. Все бизнес-приложения из "облака": от 1С до почты и телефонии - относятся к категории услуг SaaS и предоставляются по подписке. Облачный провайдер в данном случае несет ответственность за работоспособность готового конечного сервиса, а заказчик даже не знает, на каком оборудовании и с использованием какого ПО ему предоставляется доступ к конечному продукту.

Как облачный провайдер тарифицирует услуги? В случае IaaS тарификация происходит по виртуальным машинам, в случае PaaS тарификация идет по платформе, например, по количеству арендованных баз данных или по количеству операционных систем. SaaS тарифицируется сложнее всего, потому что у каждого SaaS-продукта есть свой параметр тарификации: например, в случае с почтой в "облаке" это может быть количество пользователей, количество почтовых ящиков, объем почтовых ящиков и т.д.

По объему рынка сейчас в России IaaS занимает первое место и является самой востребованной услугой. На втором месте SaaS, а на третьем месте - PaaS. Почему IaaS остается самой распространенной услугой? Наши заказчики пока отдают предпочтение своим специалистам для выполнения задач по администрированию инфраструктуры. На Западе все немного не так - там ИТ-специалисты больше занимаются сложными, специфичными задачами, необходимыми для развития конкретного бизнеса. Тем не менее, темпы роста рынка SaaS в России говорят нам о том, что модель потребления в нашей стране скоро изменится.

4.3. Электронные торговые площадки

Тендерные площадки - это интернет-порталы, где участники торгов, а именно заказчик и поставщик, взаимодействуют друг с другом с целью получить наиболее выгодные условия для осуществления сделки и заключения контракта.

Для выполнения каких-либо действий на ЭТП необходимо пройти аккредитацию на ней и оплатить использование ресурсов, если речь идет о коммерческой тендерной площадке.

Первый вид - это государственные торговые площадки. Распоряжением Правительства от 12 июля 2018 г. № 1447-р был установлен список площадок, на которых будут проводить закупки для обеспечения нужд муниципальных и федеральных учреждений. Также на этих ЭТП будут осуществляться закупки у субъектов СМП в рамках 223-ФЗ. Полноправное функционирование данные ЭТП начинают с 1 октября 2018 г.

Список данных операторов можно найти на официальном сайте. Только на этих порталах участники могут принимать участие в торгах по № 44-ФЗ РФ на госзаказы. Для того чтобы стать участником государственных торгов, не надо оплачивать никаких взносов или комиссий на ЭТП, достаточно пройти аккредитацию и получить ЭЦП, действующую на федеральной электронной площадке. Но после начала полного функционирования данных торговых площадок операторы будут взимать плату с победителя закупки.

Второй вид - коммерческие тендерные площадки. Список данных ЭТП очень широк и постоянно обновляется. Такие ресурсы чаще всего являются региональными либо отраслевыми и ведут свою деятельность в рамках № 223-ФЗ РФ. Заказы, размещаемые на них, относятся к коммерческой деятельности различных организаций, которым необходимо получить товар, услуги или работу по выгодной цене. Также на таких ЭТП проводятся закупки по банкротству, реализация арестованного имущества и т.д.

Такие площадки электронных торгов взимают определенную плату за размещение тендеров с заказчиков и за возможность участвовать в аукционе или конкурсе компаний-поставщиков. На этих порталах также необходимо пройти аккредитацию, предоставив запрашиваемые документы, и получить ЭЦП.

Появление площадок электронных торгов было обосновано тем, что они несут ряд преимуществ для всех участников:

1. Для поставщиков становится просто и быстро найти нужный тендер, они могут следить за аукционами коммерческого или госу-

дарственного оператора, экономят деньги на рекламе своего товара или услуги и могут наравне с крупными конкурентами претендовать на выигрыш электронного аукциона. Помимо всего прочего, ЭТП обеспечивают прозрачность сделки, и риск коррупционных действий становится минимальным.

2. Для заказчика выгода обусловлена тем, что ему не надо самостоятельно искать подрядчика и сравнивать условия для выбора наиболее оптимального. При размещении заказа на торговой площадке России появляется большой выбор среди поставщиков и можно выбрать наиболее выгодные условия для подписания контракта.

Во всех действиях, совершаемых на ЭТП, соблюдается законодательство Российской Федерации. Торговые площадки для аукционов обладают рядом функций:

1) выбор закупки в зависимости от выставленного фильтра;

2) просмотр тендерной документации заказчика и направление запроса на ее расшифровку;

3) собственный счет для перевода обеспечения заявки на участие в торгах, а также блокировка/разблокировка этих денежных средств;

4) проведение торговых процедур: электронных аукционов, конкурсов, запросов котировок и предложений и других (с 1 января 2019 г. все открытые процедуры будут обязаны проводиться в электронной форме на ЭТП).

Таким образом, становится понятно, что использование площадок для тендеров существенно упрощает закупочные процедуры.

Во-первых, на таких ЭТП могут принять участие поставщики со всей страны, и, соответственно, будет много предложений, среди которых заказчик может выбрать наиболее выгодное. Во-вторых, для неизвестных поставщиков это хороший шанс найти новых клиентов, предоставив выгодные условия и качественные товары или услуги, соответствующие требованиям заказчика. Важным моментом также является минимизация риска коррупции.

Электронных площадок для проведения торгов становится с каждым годом все больше, их перечень постоянно обновляется. Список основных ЭТП, работающих сейчас, можно найти в Internet. Вы можете перейти на сайт каждой из них и выбрать ту, которая вам подойдет.

Заключение

Основное средство ИКТ-технологии для информационной среды системы образования - это персональный компьютер, оснащенный необходимым программным обеспечением системного и прикладного характера, а также инструментальные средства. К системным в первую очередь относят операционный софт. Он делает возможным взаимодействие всех программ ПЭВМ с оборудованием и пользователем ПК. В данную категорию также включают сервисный и служебный софт. К прикладным программам относится обеспечение, которое представляет собой инструментарий информационных технологий - работа с текстами, графикой, таблицами и т.д. Современная система образования широко использует универсальный прикладный офисный софт и средства ИКТ, такие как текстовые процессоры, подготовка презентаций, электронные таблицы, графические пакеты, органайзеры, базы данных и т.п.

Сетевые технологии постоянно совершенствуются и изменяются. Компьютерное образование и самообразование - непрерывный процесс, и данное пособие лишь ступенька на пути к вашему персональному компьютерному образованию. С организацией компьютерных сетей и аналогичных им средств процесс образования перешел в новое качество. В первую очередь, это связано с возможностью оперативного получения информации из любой точки мира. Благодаря глобальной компьютерной сети Internet теперь возможен мгновенный доступ к информационным ресурсам планеты (электронным библиотекам, хранилищам файлов, базам данных и т.д.). В этом популярном ресурсе опубликовано более двух миллиардов различных мультимедийных документов. Сеть открывает доступ и позволяет использовать другие распространенные ИКТ-технологии, к их числу относятся группы новостей, электронная почта, чат, списки, рассылки. Кроме того, разработано специальное программное обеспечение для общения онлайн (в режиме реального времени), позволяющее после установления сеанса передавать текст (вводится с клавиатуры), а также звук, изображение и различные файлы. Такой софт дает возможность организовать совместную связь удаленных пользователей с запущенным на локальном персональном компьютере обеспечением.

Список рекомендуемой литературы

1. *Авербах, В.С.* Введение в вычислительные сети [Текст] / В.С. Авербах. - Самара : Изд-во Самар. гос. экон. ун-та, 2008. - 213 с.

2. Информационные технологии в экономике и управлении [Текст] : учеб. для академического бакалавриата / В.В. Трофимов [и др.] ; под ред. В.В. Трофимова. - 2-е изд., перераб. и доп. - Москва : Юрайт, 2016. - 482 с. - (Бакалавр. Академический курс).

3. *Винстон, У.Л.* Microsoft Excel 2013. Анализ данных и бизнес-моделирование [Электронное издание]. - Москва : Русская редакция, 2015. - 864 с.

4. *Медведев, А.* Облачные технологии: тенденции развития, примеры исполнения / А. Медведев // Современные технологии автоматизации. - 2013. - № 2. - С. 6-9.

5. Эталонная архитектура облачных вычислений [Текст] : рекомендации Национального института стандартов и технологий (США). - 2007. - NIST; USA.

6. Уголовный кодекс РФ. Статья 159.6. : федер. закон от 29.11.2012 № 207-ФЗ [Электронный ресурс] : [ред. от 13.10.2018]. - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/51c53d82b60ac8c009745bdea3838d507064c6d3/.

7. Internet Fraud [Электронный ресурс]. - Режим доступа: https://en.wikipedia.org/wiki/Internet_fraud.

8. Научная электронная библиотека ELIBRARY.RU [Электронный ресурс]. - Режим доступа: http://elibrary.ru.

9. http://fb.ru/article/145313/informatsionno-kommunikatsionnaya-tehnologiya-ikt-tehnologii.

Учебное издание

Чеверева Светлана Александровна

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие
для студентов вузов

Руководитель издательской группы О.В. Егорова
Редактор Т.В. Федулова
Корректор Л.И. Трофимова
Компьютерная верстка - Д.В. Жоголева

Подписано к изданию 27.12.2018. Печ. л. 5,94.
ФГБОУ ВО "Самарский государственный экономический университет".
443090, Самара, ул. Советской Армии, 141.